CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Homeland Security Committee

Countering Threats Posed by the Chinese Communist Party to U.S. National Security

CRAIG SINGLETON

China Program Senior Director and Senior Fellow
Foundation for Defense of Democracies

With contributions from Jack Burnham, M. Reece Breaux, and Kirin Atluru

Washington, DC
March 5, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chinese Communist Party Chairman Xi Jinping has declared technological innovation the "main battlefield" in China's quest for global preeminence.[1] For Xi, Chinese-style modernization is not merely an economic goal — it is a historic mandate with global implications. In aiming to dominate what he calls "new productive forces" (新质生产力) — breakthroughs in batteries, biotech, LiDAR, drones, and other cutting-edge technologies — Xi seeks to cement Chinese control over the drivers of the next industrial revolution.[2] In doing so, Xi intends to transform China into a global science superpower.[3]

Yet Xi's strategy rests on a glaring vulnerability. It hinges on sustained access to U.S. capital markets and advanced technology, as well as near-unfettered reach into American data and critical infrastructure systems. On this front, policymakers must act decisively and without delay, as Xi's ambitions pose an unprecedented threat to U.S. homeland security.

Xi's broader technological ambitions underpin China's military-civil fusion (军民融合) strategy, which breaks down barriers between military and civilian institutions to mobilize the latter in service of the former.[4] Military-civil fusion accelerates the direct transfer of data and advanced technologies — be they biotech discoveries or next-generation batteries — straight into China's defense sector. As a result, China's People's Liberation Army's (PLA) capabilities keep pace with rapid civilian technological progress, expanding Beijing's ability to challenge American interests at home and abroad.

Beijing's strategy is unfolding in three interlocking phases. First, Chinese actors and companies are relentlessly penetrating U.S. networks and critical infrastructure. Hacking campaigns like Salt, Volt, and Flax Typhoon demonstrate how state-sponsored entities are infiltrating our digital ecosystems to steal sensitive data and embed themselves in our communications, industrial, and defense networks.[5] These intrusions serve dual purposes: They collect intelligence and prepare for future sabotage. More than a year after these breaches were first made public, China still maintains persistent access to many compromised networks, having faced almost no penalty for its actions.

Second, Beijing prepositions its advantages by engineering dependencies that can be weaponized to advance China's national interests. China deliberately creates choke points in global supply chains and network infrastructures. Chinese-made LiDAR, compromised cranes in U.S. ports, and drones in both civilian and military applications illustrate this approach. Moreover, the U.S.

---

[1] "加快建设科技强国 实现高水平科技自立自强 [Accelerating the Construction of a Science and Technology Powerhouse and Achieving High-Level Scientific and Technological Self-Reliance and Self-Reliance]," *Qiushi*, April 30, 2022. (https://archive.ph/pAqWG)

[2] Craig Singleton and Amaya Marion, "Safeguarding U.S. Interests in the Face of China's 'New Productive Forces' Strategy," *Foundation for Defense of Democracies*, May 2, 2024. (https://www.fdd.org/analysis/2024/05/02/safeguarding-u-s-interests-in-the-face-of-chinas-new-productive-forces-strategy); Arendse Huld, "China's New Quality Productive Forces: An Explainer," *China Briefing*, September 2, 2024. (https://www.china-briefing.com/news/chinas-new-quality-productive-forces-an-explainer)

[3] Ben Murphy, Rogier Creemers, Elsa Kania, Paul Triolo, and Kevin Neville, "Xi Jinping: 'Strive to Become the World's Primary Center for Science and High Ground for Innovation,'" *Stanford Cyber Policy Center*, March 18, 2021. (https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-science-and-high-ground-for-innovation/#fn1)

[4] U.S. Department of State, "The Chinese Communist Party's Military-Civil Fusion Policy," 2020. (https://2017-2021.state.gov/military-civil-fusion)

[5] Craig Singleton, "Securing Communications Networks from Foreign Adversaries," *Testimony before the House Committee on Energy and Commerce*, February 15, 2024. (https://docs.house.gov/meetings/IF/IF16/20240215/116856/HMTG-118-IF16-Wstate-SingletonC-20240215.pdf)

Defense Department has warned that Beijing's cyber activities aim not merely to monitor but to compromise — and ultimately control — these sensitive systems and defense-related supply chains.[6] Whether it's biotech integrated into healthcare and defense or batteries powering our energy grid, each dependency represents a strategic vulnerability that endangers U.S. national security.[7]

Third, Beijing profits from this dual approach. The economic and military gains are immense. Chinese exports in high-tech sectors fuel rapid PLA modernization and undercut global competitors.[8] Every infiltration and dependency generates revenue that China reinvests in military-civil fusion programs, enhancing its capacity to wage war. By consistently converting market access into geopolitical leverage, the Chinese Communist Party (CCP) has significantly strengthened its influence over U.S. and allied decision-making, with the goal of weaponizing Western reliance on these technologies to force countries into accepting its strategic demands.

Today's stakes have never been higher. Beijing's three-phase strategy — penetrating our networks, prepositioning technological choke points, and profiting from those dependencies — poses a direct challenge to U.S. homeland security. In response, the United States must both fortify its networks and curtail China's ability to exploit these vulnerabilities to achieve its desired strategic ends. That effort demands robust outbound investment screening, paired with technology-specific controls and procurement bans, to safeguard America's critical infrastructure and national interests.

In sum, China's strategy threatens not only our technological edge but the security of our nation. As we enter an era of intensified great-power competition, policymakers must remain clear-eyed about the acute risks posed by Beijing's far-reaching ambitions and take immediate action to safeguard America's homeland security, preserve our leadership in innovation, and secure a free and open global order.

I. Xi's Strategic Vision for Technological Dominance

Xi regards technological prowess as the core pillar of China's "comprehensive national security" concept.[9] He has broadened the concept of security to encompass not only military strength but also the economic, political, and societal realms. In this framework, leading-edge technology undergirds everything from sustaining economic vitality to upholding the Communist Party's repressive surveillance apparatus. Although Xi acknowledges that China remains partially

[6] "Summary of the 2023 Department of Defense Cyber Strategy," U.S. Department of Defense, accessed February 13, 2024. (https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF)

[7] Craig Singleton, "Biotech Battlefield: Weaponizing Innovation in the Age of Genomics," *Foundation for Defense of Democracies*, January 15, 2025. (https://www.fdd.org/analysis/2025/01/15/biotech-battlefield); Craig Singleton, "Beijing's Power Play; Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries," *Foundation for Defense of Democracies*, October 23, 2023. (https://www.fdd.org/analysis/2023/10/23/beijings-power-play)

[8] CEIC Data, "How High-Tech Has Taken a Greater Share of China's Exports," *CEIC Data*, 2024. (https://info.ceicdata.com/how-high-tech-has-taken-a-greater-share-of-chinas-exports); The Office of Senator Marco Rubio, "The World China Made: 'Made in China 2025' Nine Years Late," *Project for Strong Labor Markets and National Development*, 2024. (https://www.americanrhetoric.com/speeches/PDFFiles/Marco-Rubio-The-World-China-Made.pdf)

[9] Sheena Chestnut Greitens, "Xi's Obsession: Why China Is Digging In at Home and Asserting Itself Abroad," *Foreign Affairs*, July 28, 2023. (https://www.foreignaffairs.com/united-states/xis-security-obsession); Sheena Chestnut Greitens, "Internal Security & Grand Strategy: China's Approach to National Security under Xi Jinping," Statement before the U.S.-China Economic & Security Review Commission Hearing on "U.S.-China Relations at the Chinese Communist Party's Centennial," Panel on "Trends in China's Politics, Economics, and Security Policy," January 28, 2021. (https://www.uscc.gov/sites/default/files/2021-01/Sheena_Chestnut_Greitens_Testimony.pdf)

dependent on foreign technology, he has repeatedly warned that such reliance creates "stranglehold" (卡脖子) vulnerabilities, framing the pursuit of self-reliance as a matter of national survival.[10] His speeches emphasize that advanced fields like artificial intelligence, quantum computing, and biotech will determine the balance of global power in the decades ahead.

To realize this vision, Xi calls for fusing China's military and civilian capabilities into a single innovation engine. Under this strategy, state-backed companies and research institutes operate as dual-use platforms, ensuring that breakthroughs in commercial sectors directly benefit the PLA, as well as China's intelligence and security agencies. In Xi's view, this synergy not only accelerates military modernization but also positions China as a global technology leader. Official policies such as Made in China 2025 and China's most recent 14th Five-Year Plan mandate state involvement in strategic industries, from robotics and electric vehicles to high-performance computing.[11] By consolidating resources under CCP oversight, Xi believes China can outpace Western rivals and dictate the global technology agenda.

Global Leadership of Select Strategic Technologies, 2019-2023

Strategic Technology	Global Leader
Natural Language Processing	United States
Quantum Computing	United States
Advanced Aircraft Engines	China
Drones, Swarming, and Collaborative Robotics	China
Electric Batteries	China
Photovoltaics	China
Genetic Engineering	United States
Synthetic Biology	China

[10] "China Focus: Xi calls for developing China into world science and technology leader," *Xinhua* (China), May 28, 2018. (http://www.xinhuanet.com/english/2018-05/29/c_137213175.htm)

[11] China National People's Congress, "中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 (Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035)," May 13, 2021. (https://cset.georgetown.edu/publication/china-14th-five-year-plan); The Office of Senator Marco Rubio, "The World China Made: 'Made in China 2025' Nine Years Late," *Project for Strong Labor Markets and National Development*, 2024. (https://www.americanrhetoric.com/speeches/PDFFiles/Marco-Rubio-The-World-China-Made.pdf)

Hypersonic Detection and Tracking	China
Electronic Warfare	China

Source: *Australian Strategic Policy Institute*

An equally critical dimension of Xi's vision involves shaping international standards and norms. He has instructed Chinese firms and state agencies to take active roles in global standards-setting bodies, from the International Telecommunication Union (ITU) to the International Organization for Standardization (ISO).[12] By championing proprietary Chinese solutions — ranging from next-generation wireless protocols to AI ethics frameworks — Beijing seeks to establish global rules that align with its domestic priorities. Xi has underscored that controlling these technical rules of the game enhances China's ability to project influence abroad, effectively rewriting the architecture of global trade and communication to suit national interests.

At home, Xi's strategic vision also serves the CCP's political imperatives. The push for self-reliance in semiconductors, batteries, and other high-tech components reinforces state control over critical supply chains, reducing the risk that foreign sanctions or embargoes could undermine Chinese stability. Xi's domestic rhetoric frequently underscores that lagging behind in core technologies endangers both economic development and the Party's leadership. By placing key industries under direct Party supervision, Xi aims to ensure that private innovation does not become a breeding ground for dissent or foreign infiltration. This approach strengthens the Party's grip while speeding the pace of scientific discovery.

In tandem, Xi's ambitions extend well beyond China's borders. He frames technology not only as a means to catch up with advanced nations but also to surpass them, thereby reshaping global governance. From establishing digital payment systems that bypass Western financial networks to exporting surveillance platforms that promote a model of digital authoritarianism, Xi's strategy weds technology with foreign policy.[13] He portrays these exports as symbols of Chinese ingenuity, persuading other countries — especially in the Global South — to adopt Chinese standards and technology.[14] By weaving technology into broader diplomatic efforts, Xi solidifies Beijing's position as an alternative pole to the U.S.-led system.

[12] "China is writing the world's technology rules," *The Economist*, October 8, 2024. (https://www.economist.com/business/2024/10/10/china-is-writing-the-worlds-technology-rules); Matt Sheehan and Jacob Feldgoise, "What Washington Gets Wrong About China and Technical Standards," C*arnegie Endowment For International Peace*, February 27, 2023. (https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en)
[13] Barry Eichengreen, "Sanctions, SWIFT, and China's Cross-Border Interbank Payments System," *Center for Strategic & International Studies*, May 20, 2022. (https://www.csis.org/analysis/sanctions-swift-and-chinas-cross-border-interbank-payments-system)
[14] Bulelani Jili, "China's surveillance ecosystem and the global spread of its tools," *Atlantic Council*, October 17, 2022. (https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools)

These goals carry profound implications for U.S. homeland security and the global order at large. Xi's pursuit of technological dominance does not merely aim to strengthen China's economy; it seeks to reposition Beijing as the central architect of tomorrow's innovations, standards, and norms. While such objectives might appear purely aspirational, Xi's conception of "comprehensive national security" makes clear that technology leadership is also a means of political control and strategic leverage.[15] In short, Xi's vision threatens to remake the balance of power across critical sectors — from artificial intelligence to quantum computing — in ways that could challenge not only American competitiveness but also the security and freedom of open societies worldwide.

II. Penetrating U.S. Networks and Critical Infrastructure

China's move from high-level technological aspirations to tangible action began with a systematic push to penetrate U.S. networks and critical infrastructure. This effort has been neither opportunistic nor ad hoc; rather, it reflects a methodical plan to gather intelligence, undermine American defenses, and engineer dependencies that can be weaponized during both peace and wartime. Beijing's infiltration extends beyond mere data theft, delving into the very architecture of U.S. supply chains and physical systems in order to secure both economic and strategic leverage.

In the cyber domain, Chinese state-sponsored hackers routinely breach U.S. digital ecosystems. Campaigns such as Salt, Volt, and Flax Typhoon demonstrate the sophistication with which these actors exploit software and hardware vulnerabilities, implant malicious code, and maintain persistent access — even after detection.[16] According to warnings from the Department of Homeland Security (DHS), the Federal Bureau of Investigation, and the National Security Agency, these persistent footholds enable China to exfiltrate vast amounts of sensitive information — ranging from the contents of phone calls to proprietary corporate data — and lay the groundwork for future sabotage.[17] Minimal repercussions have only emboldened these activities, leaving unpatched vulnerabilities across defense and industrial networks.

Select PRC Cyber Intrusions, 2024-2018

Year	PRC Hacking Incident	Target
December 2024	Third-Party Vendor to U.S. Treasury Department	U.S. Treasury Department; Office of Foreign Assets; Control; Committee of Foreign Investment in the United States

[15] Katja Drinhausen and Helena Legarda, "'Comprehensive National Security' unleashed: How Xi's approach shapes China's policies at home and abroad," *Mercator Institute for China Studies*, September 15, 2022. (https://merics.org/en/report/comprehensive-national-security-unleashed-how-xis-approach-shapes-chinas-policies-home-and)

[16] House Committee on Homeland Security, "Cyber Threat Snapshot," November 12, 2024. (https://homeland.house.gov/wp-content/uploads/2024/11/11.12.24-Cyber-Threat-Snapshot.pdf)

[17] U.S. Department of Justice, "Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers," September 18, 2024. (https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a); Matt Kapko, "Feds raise alarm on China-linked infiltration of telecom networks," *Cybersecurity Drive*, December 4, 2024. (https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576)

November 2024	Salt Typhoon	Telecommunications providers
September 2024	Flax Typhoon	Communications infrastructure; government agencies; critical infrastructure
May 2023	Volt Typhoon	Critical infrastructure
July 2023	Microsoft Email System	U.S. State Department; U.S. Commerce Department
May 2023	Guam	U.S. communications network
December 2022	U.S. Small Business Administration	U.S. COVID-19 relief funds
May 2022	U.S. private sector	Intellectual property from unidentified U.S. and European firms
October 2020	U.S. defense industrial base	Military secrets and intellectual property from unidentified U.S. firms
April 2020	U.S. healthcare system	Hospitals; pharmaceutical manufacturers; U.S. Department of Health and Human Services
March 2019	General Electric	Advanced aircraft engine designs
December 2018	U.S. defense industrial base	U.S. Navy contractors; ship maintenance data; missile plans

Source: Source: Cybersecurity and Infrastructure Security Agency China State-Sponsored Cyber Threat Advisories

Beijing's penetration strategy also targets the operational technology systems that undergird America's physical infrastructure. Devices like advanced LiDAR sensors, surveillance cameras, and drones — often from well-known Chinese brands — are embedded in energy grids, transportation networks, and industrial control systems.[18] By intertwining themselves with these systems, Chinese entities gain a vantage point over vital operations essential to U.S. homeland security. U.S. Department of Defense officials have voiced particular concern about Chinese influence over battery production, underscoring how reliance on these supply chains may grant

[18] Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024. (https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems); Nik Martin, "US bans Chinese telecom, surveillance cameras," *DW News*, November 26, 2022. (https://www.dw.com/en/us-bans-chinese-telecom-surveillance-cameras/a-63895206); Ana Swanson, "U.S. Weighs Ban on Chinese Drones, Citing National Security Concerns," *The New York Times*, January 2, 2025. (https://www.nytimes.com/2025/01/02/us/politics/drone-ban-china-security.html)

Beijing the power to disrupt or delay critical functions during a crisis.[19] A 2025 DHS bulletin warned that internet-connected cameras manufactured in China could potentially be exploited for espionage targeting the nation's critical infrastructure installations.[20]

Such infiltration does not end with a simple presence in foreign networks; it aims to transform global supply chain interdependence into a geopolitical weapon. China deliberately fosters reliance on its technology in advanced manufacturing, biotech, and other high-tech arenas, thereby creating strategic choke points. Dominance by Chinese battery giants like CATL and drone manufacturers like DJI exemplifies how entire U.S. industries — from automotive to agriculture — can become dependent on PRC-sourced parts and devices.[21] In a crisis, Beijing could withhold exports, inflate prices, or insert malicious features, effectively coercing U.S. decision-makers. Rather than hide their origins, these recognized Chinese brands benefit from market leadership, which makes it easier for them to entrench themselves in U.S. supply chains.

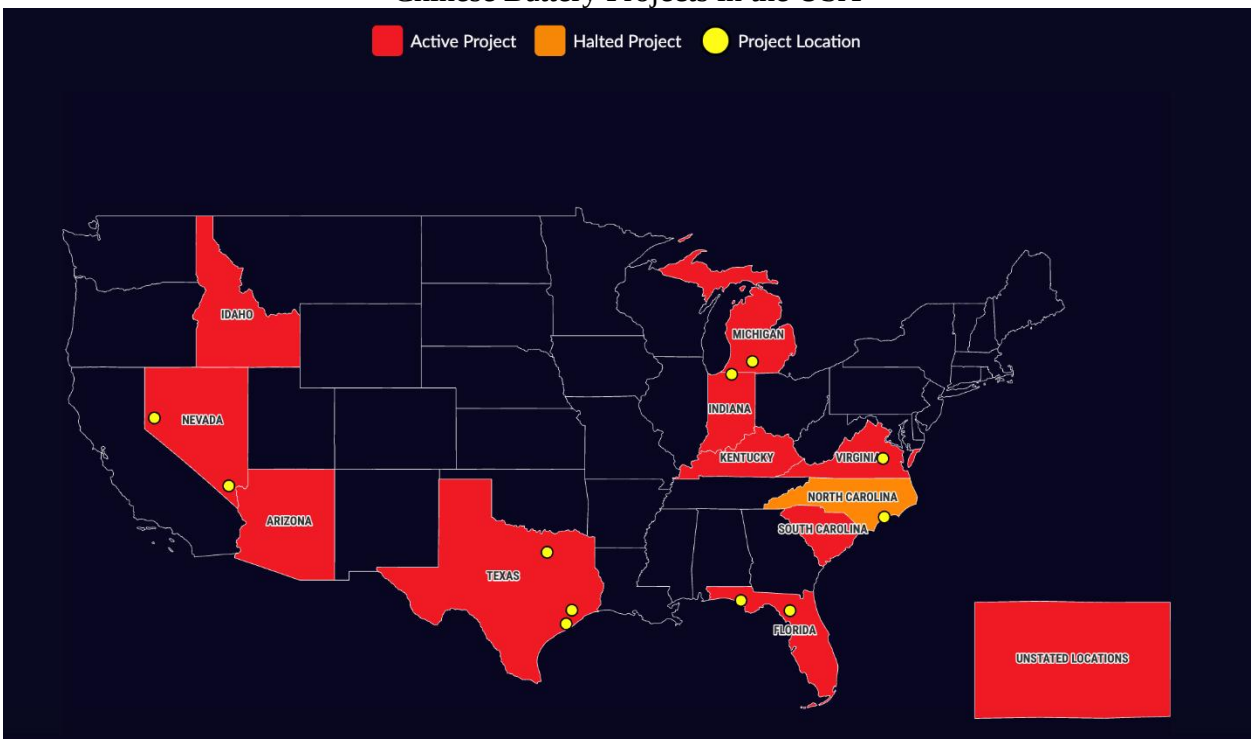
Leading Global Chinese Technology Firms

Industry	Chinese Champion	Global Market Share (%)
Drones	DJI	90
Batteries	CATL	38
Electric Vehicles	BYD	20
Agricultural Technology	Syngenta*	60
LiDAR	Hesai	47
Genomics	BGI Genomics**	5.8
Solar	Tongwei Solar	28

Source: *MIT Technology Review; South China Morning Post; International Energy Agency; Fitch Ratings; Yole Group; SanDiegomics; Fitch Ratings*
*Accounts for share of crop protection market
**Accounts for share of global sequencing market

[19] Ellen Nakashima, "Pentagon Adds Chinese Technology Firms to Blacklist over Security Concerns," *The Washington Post*, January 6, 2025. (www.washingtonpost.com/national-security/2025/01/06/pentagon-blacklist-china-technology-ev)
[20] "People's Republic of China: Exploitation of Internet-Connected Cameras Threatens US Critical Infrastructure," Department of Homeland Security, February 3, 2025. (https://wwema.org/wp-content/uploads/2025/02/Cybersecurity-DHS-IA-IF-2025-Peoples-Republic-of-China-Exploitation-of-Internet-Connected-Cameras.pdf)
[21] Craig Singleton, "Chinese Battery Behemoth CATL: U.S. Sites and Operations," *Foundation for Defense of Democracies*, 2023. (https://www.fdd.org/catlinusa)

Chinese Battery Projects in the USA



Source: "Chinese Battery Behemoth CATL: US Sites and Operations," *Foundation for Defense of Democracies*

The breadth of Beijing's penetration becomes evident when examining the key sectors at risk. In biotech and advanced manufacturing, Chinese firms infiltrate global research networks to acquire sensitive data that accelerates both civilian medical breakthroughs and PLA modernization. In energy and battery technologies, controlling production lines allows Beijing to create potential choke points in electric grids and vehicle fleets, leaving essential infrastructure vulnerable. In drones and autonomous systems, Chinese-made models integrate seamlessly into U.S. surveillance and logistics, opening covert pathways for data exfiltration or sabotage.

Similarly, in LiDAR and sensor technologies, Chinese devices capture real-time data from both smart city systems and military reconnaissance operations, enabling potential manipulation of critical monitoring functions. And, in surveillance cameras, millions of PRC-manufactured units — sometimes rebranded under U.S. labels — now secure airports, ports, and government buildings, raising concerns about remote access and unauthorized data extraction.

By embedding themselves in both digital networks and physical supply chains, Chinese entities gain unmatched visibility and control over critical U.S. systems. Each compromised link — be it a software backdoor or a key hardware component — adds another layer of risk. In a time of heightened tension, Beijing could exploit these vulnerabilities to disrupt communications, sabotage power grids, cripple ground transportation, or undermine emergency services.

Persistent intrusions also feed China's broader intelligence apparatus, sharpening its ability to plan and execute more sophisticated operations in the future.

Despite the seriousness of these breaches, Beijing has faced few consequences for these infiltrations. The absence of strong countermeasures only emboldens Chinese cyber actors and commercial giants to expand their presence. Moreover, repeated intrusions with minimal pushback allow Chinese cyber actors to refine their tactics, leaving critical networks and supply chains increasingly exposed. Over time, unchecked infiltration erodes America's ability to protect its own infrastructure, maintain a technological edge, and respond effectively to emergencies.

Ultimately, China's penetration of U.S. networks and infrastructure — coupled with its deliberate manipulation of weaponized supply chains — demands a forceful and multi-layered response. Policymakers must recognize that each infiltration is not just a theft of data but also a strategic maneuver to secure leverage during future conflicts or crises. Fortifying networks, scrutinizing outbound investments, and collaborating with trusted allies to rebuild resilient supply chains constitute the first steps in mitigating these threats. If left unaddressed, Beijing's penetration strategy will continue to undermine U.S. homeland security, national defense, and economic competitiveness — key pillars of American strength in the 21st century.

III. Prepositioning: Laying the Groundwork for Crisis Manipulation

China's infiltration of U.S. networks and infrastructure lays the groundwork for something more potent than mere data theft: prepositioning. Once embedded in vital systems, Beijing can do more than collect intelligence — it can prepare the battlefield for future crises by creating doubts about the reliability of America's own infrastructure.[22] This tactic reflects a guiding principle in PLA doctrine, which stresses that "the boundary between war and peace is fluid," and that forward-placed cyber and physical footholds allow China to gain mastery well before overt conflict begins. The concept resonates with the PLA's principle of xianfa zhiren (先发制人), or "gaining mastery by striking first," whereby effective prepositioning can degrade an adversary's defenses even in peacetime.[23]

Indeed, Xi's broader vision of "winning without fighting" finds direct application here: Infiltration itself can yield strategic victories by stalling or preventing U.S. action at critical junctures.

At its core, prepositioning transforms infiltration from an intelligence windfall into a means of exerting leverage when tensions escalate. If U.S. officials suspect that a communications network, electric grid, or drone fleet has been compromised, they may hesitate to rely on those assets in an emergency. The mere possibility of sabotage can induce self-imposed restrictions, effectively degrading America's crisis response. PLA theorists emphasize that instilling doubt in

[22] David DiMolfetta, "Chinese Hackers Embedded in U.S. Networks for Years, Pre-Positioning for Future Attacks, IC Warns," *NextGov*, February 7 2024. (https://www.nextgov.com/cybersecurity/2024/02/chinese-hackers-embedded-us-networks-years-pre-positioning-future-attacks-ic-warns/394009)

[23] James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David Frelinger, David C. Gompert, Martin C. Libicki, and Kevin L. Pollpeter, "Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense," *RAND Corporation*, accessed February 26, 2025. (https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG340.pdf)

an adversary's capabilities is often as effective as physical destruction.[24] By eroding confidence in U.S. systems, Beijing can blunt Washington's willingness to act decisively without firing a shot.

This prepositioning extends beyond code lurking in server backdoors; it includes the manipulation of hardware and supply chains that Beijing has painstakingly embedded in key industries. Chinese-manufactured batteries, LiDAR devices, and rebranded surveillance cameras can be remotely updated to alter their functionality at will.[25] Such hidden capabilities need not be activated frequently — only at moments when disruption is most advantageous to Beijing's strategic aims. In effect, these sleeper threats align with Xi's emphasis on achieving strategic objectives without direct conflict, using targeted interference or withheld components to stall American mobilization or sow confusion in the midst of a crisis.

The ramifications become even more acute if a conflict with China turns kinetic. In that scenario, prepositioned exploits could allow Beijing to degrade U.S. command-and-control functions at the outset of hostilities, paralyzing the rapid deployment of American forces or neutralizing critical logistics hubs. Military communications satellites, drone fleets, and other high-value transportation platforms might be disabled or manipulated, sowing confusion at a critical moment. Such disruptions could produce a cascading effect, crippling not only frontline operations but also broader U.S. infrastructure — such as port facilities and energy grids — on which those operations depend.

By compromising both military and civilian networks in advance, Beijing aims to slow the U.S. response, shift the balance of power early in the conflict, and potentially force a negotiated outcome favorable to Chinese interests.

From a homeland security perspective, prepositioning poses grave concerns because it exploits vulnerabilities that appear benign in ordinary times.[26] A port's container cranes, a municipal drone fleet, or even a hospital's medical equipment might operate smoothly for years — until a crisis. At that pivotal moment, compromised systems can fail, or merely be perceived as compromised, forcing operators to revert to slower, less capable backups. This dynamic extends China's influence well beyond direct confrontation, granting Beijing a silent veto over America's rapid-response capabilities.

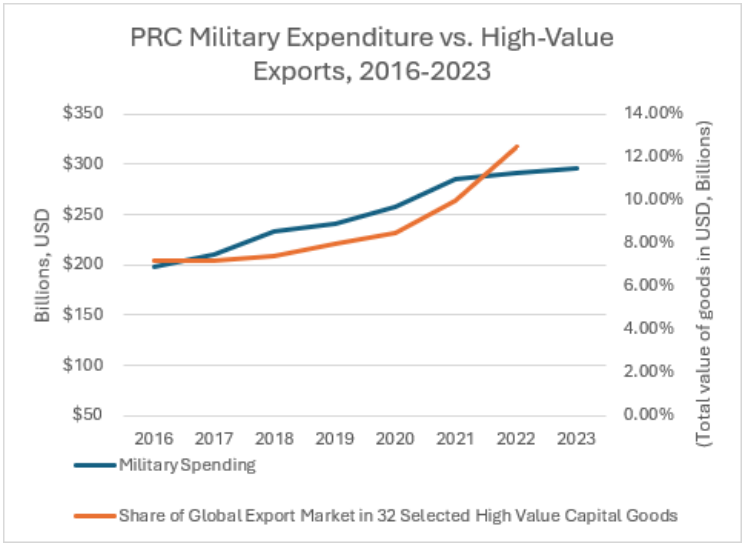
Ultimately, prepositioning is the logical outcome of Beijing's infiltration efforts; penetration itself is not the end goal but rather the vehicle through which China creates latent threats in both digital networks and physical supply chains. By embedding malicious capabilities — ranging from dormant software code to critical hardware vulnerabilities — Beijing gains the ability to

[24] Jeffery Engstrom, "Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare," *RAND Corporation*, February 1, 2018. (https://www.rand.org/pubs/research_reports/RR1708.html)
[25] Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024. (https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems); Craig Singleton, "Targeting Tiandy," *Foundation for Defense of Democracies*, December 1, 2022. (https://www.fdd.org/analysis/2022/12/01/targeting-tiandy)
[26] U.S. Department of Homeland Security, Cybersecurity Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)

shape U.S. decision-making under duress. This capacity to degrade or disable key systems stands at the heart of Xi's vision for leveraging technology as a geopolitical tool.

IV. Profiting from Dependencies

Beijing's strategy of penetrating and prepositioning within U.S. networks is not solely about intelligence gathering — it is also designed to generate substantial economic leverage. Chinese high-tech exports, ranging from advanced sensors and biotech innovations to drones and surveillance systems, generate billions of dollars in revenue each year.[27] Major companies like DJI and CATL, for example, report multi-billion-dollar revenues bolstered by strong state support through subsidies, low-interest loans, and favorable industrial policies.[28] These financial gains are reinvested in research and development and military modernization, fueling the PLA's rapid expansion and creating a self-reinforcing cycle of power.



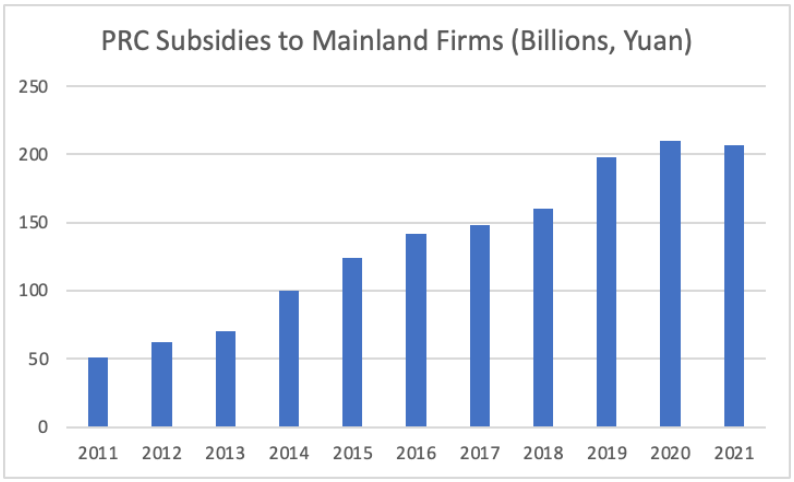
Source: Wall Street Journal; Statista; Department of Defense; Huawei; World Bank

By embedding its technology in critical supply chains, Beijing forces entire U.S. industries — from automotive and energy to healthcare and agriculture — to depend on Chinese components.[29] This dependency not only drives significant revenue for Chinese firms but also undermines American competitiveness. When U.S. companies rely on state-backed Chinese technology, market access transforms into a strategic vulnerability. In a crisis, Beijing could disrupt these supply chains by halting exports, manipulating pricing, or even inserting malicious features — thereby coercing U.S. decision-makers and weakening our economic foundation.

Chinese enterprises operating in key high-tech sectors benefit from extensive state backing. Favorable policies and direct financial support enable companies like CATL, DJI, and leading

[27] The State Council, The People's Republic of China, "Chinese Software and Info-Tech Sector Reports Revenue, Profit Growth in 2023," January 27, 2024. (https://english.www.gov.cn/archive/statistics/202401/27/content_WS65b48d3fc6d0868f4e8e3930.html)
[28] Curtis J. Milhaupt and Li-Wen Lin, "We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China," *Stanford Law Review*, 2013. (https://law.stanford.edu/publications/we-are-the-national-champions-understanding-the-mechanisms-of-state-capitalism-in-china)
[29] David Song-Penhamberger, "Controlling Tomorrow: China's Dominance Over Future Strategic Supply Chains," *The Diplomat*, August 21, 2024. (https://thediplomat.com/2024/08/controlling-tomorrow-chinas-dominance-over-future-strategic-supply-chains)

biotech firms to dominate global markets. Their commercial success translates into significant resources that Beijing channels into further technological innovation and military-civil fusion initiatives. In effect, every dollar earned through these channels not only strengthens China's economy but also reinforces its capacity to wage hybrid warfare and shape global standards.



Source: *Fitch Ratings*

Ultimately, converting market access into geopolitical leverage undermines U.S. competitiveness and national security. By profitably exploiting these dependencies, the CCP secures a dual advantage — reinforcing domestic military strength while exerting economic and diplomatic pressure on its adversaries. Disrupting these profit channels through robust export controls, stringent investment screening, and coordinated international measures is essential for protecting American industry and preserving our technological edge on the global stage.

V. Policy Recommendations

Beijing's systematic penetration of U.S. networks, its ability to preposition latent threats, and its profiteering from global dependencies underscore the urgency of a decisive policy response. The House Homeland Security Committee, in coordination with other congressional committees and executive agencies, can play a pivotal role in shaping legislation, funding priorities, and oversight mechanisms that protect America's critical infrastructure and strategic industries.

Below are key recommendations:

Overarching Measures for Homeland Security

- **Legislate Comprehensive Outbound Investment Screening, Enhanced Export Control Enforcement, and Targeted Sanctions:** Enact laws that rigorously scrutinize U.S. capital flows into Chinese firms involved in national security technologies and impose targeted sanctions on entities tied to military modernization or state surveillance — ensuring American investments do not bolster Beijing's coercive capabilities. Such a measure, modeled on the principles underpinning the

COINS Act, would ensure that American investments do not bolster Beijing's coercive capabilities, while protecting vital U.S. interests.

- **Close Export and Transshipment Loopholes:** Mandate interagency coordination among the Departments of Homeland Security, Commerce, State, Treasury, and Defense to track and penalize the rerouting of problematic Chinese technologies through third countries, with regular updates to the House Homeland Security Committee to track enforcement.

- **Establish a Critical Infrastructure Supply Chain Registry:** Direct the Department of Homeland Security to create a national registry that identifies critical components in high-risk sectors (energy, healthcare, transportation) and flags Chinese-linked vendors or products, thereby enhancing visibility into potential choke points.

- **Mandate Disclosure and Reporting for Chinese-Linked Components:** Require critical infrastructure operators to report within 72 hours any discovery of Chinese-manufactured or influenced hardware or software in sensitive systems, ensuring rapid federal response to potential infiltration.

- **Enhance Transparency for Chinese-Owned or -Controlled Firms:** Require clear labeling of high-tech products with ties to Chinese state-owned or military-linked companies — similar to existing FCC rules — so that government agencies and private operators can make informed procurement decisions and avoid hidden dependencies.

LiDAR and Sensor Technologies

- **Require DHS-Led Risk Certification:** Mandate that any LiDAR or sensor system intended for critical infrastructure (e.g., ports, airports, traffic control) undergo a DHS certification process verifying supply chain integrity and firmware security.

- **Conduct Supply Chain Audits for LiDAR Imports:** Direct DHS and the Department of Commerce to audit LiDAR and sensor imports, focusing on firmware vulnerabilities, Chinese ownership stakes, and potential remote-update backdoors.

- **Establish Sector-Specific Cybersecurity Standards:** Instruct the National Institute of Standards and Technology (NIST), in coordination with the Cybersecurity and Infrastructure Security Agency, to develop cybersecurity standards for LiDAR used in traffic management, smart cities, and other critical applications. Congress can pass legislation mandating compliance for federal contractors and grant recipients.

- **Mandate Regular Penetration Testing:** Require both public- and private-sector LiDAR users to perform periodic penetration testing and cybersecurity audits, potentially via amendments to the Federal Information Security Modernization Act (FISMA) to cover connected systems like LiDAR.

- **Ban DHS and Executive Agency Procurement of Chinese LiDAR Sensors:** Enact legislation prohibiting DHS and other federal agencies from procuring LiDAR systems manufactured by entities based in foreign countries of concern, ensuring no federal funds support risky vendors.

- **Enforce Strict LiDAR Data Localization:** Stipulate that LiDAR data collected by federal, state, or local governments be stored on U.S. soil, minimizing the risk of data exfiltration. Lawmakers could amend existing statutes (e.g., the CLOUD Act) to include LiDAR-specific data localization requirements.

- **Create a National Framework for LiDAR Data Security:** Direct the Department of Transportation (DoT), in coordination with the Transportation Security Administration (TSA) at DHS, to develop a framework governing LiDAR data in autonomous vehicles and transportation systems, mandating encryption standards, data retention policies, and data-sharing restrictions.

- **Evaluate Procurement Bans:** Consider legislation barring the Department of Transportation, DHS, and other government agencies from purchasing LiDAR sensors manufactured by companies in foreign countries of concern. This would also prevent Transportation grants (e.g., SMART Grants) from funding the acquisition of high-risk PRC-produced LiDAR systems.

- **Increase and Enforce Section 301 Tariffs on Chinese LiDAR:** Instruct the U.S. trade representative to raise tariffs on LiDAR imports from China above the current 25 percent threshold, while Customs and Border Protection conducts retroactive investigations to ensure proper enforcement and deter predatory pricing.

- **Create a DHS Task Force on Emerging LiDAR Threats:** Direct DHS, via CISA, to form an inter-agency task force dedicated to identifying and mitigating threats to LiDAR systems in transportation and critical infrastructure. Require the task force to issue regular public updates on vulnerabilities, mitigation strategies, and incident response.

- **Expand the FCC 'Covered List' to Include Chinese LiDAR Manufacturers:** Request DHS coordinate with the Federal Communications Commission to add major Chinese LiDAR producers to the "Covered List" of banned entities, blocking federal subsidies for their products and prompting a legislative review if necessary.

Batteries and Energy Technologies

- **Authorize a Comprehensive Intelligence Assessment of CATL and China's EV Industry:** Direct the intelligence community to assess the overlap between Chinese battery/EV firms (e.g., CATL, Gotion, etc.) and the Chinese Military-Industrial Companies List, as well as vulnerabilities in U.S. charging networks and energy storage systems that Beijing could exploit.

- **Institute Rigorous Regulatory Measures and Oversight Protocols:** Require federal and, where relevant, state authorities to monitor technology transfers, scrutinize investments, and ensure Chinese EV and grid-related projects adhere to stringent security and industry standards in the United States.

- **Ban DHS Procurement of Batteries from PRC-Aligned Companies:** Pass legislation prohibiting DHS and its agencies from purchasing battery systems produced by Chinese manufacturers such as CATL, BYD, Envision Energy, EVE Energy, Hithium, and Gotion High-Tech.

- **Expand CFIUS Review for Chinese Battery Investments:** Empower the Committee on Foreign Investment in the United States to more thoroughly review, limit, or condition investments by Chinese battery and EV firms in critical U.S. infrastructure or industries.

- **Strengthen Licensing Requirements for Chinese Energy Firms:** Mandate that Chinese companies operating in the U.S. energy sector undergo enhanced security reviews before receiving operational licenses, ensuring that potential risks to the grid or other vital systems are mitigated.

Biotech

- **Establish a Congressional Biotech and National Security Task Force**: Create a dedicated body to track threats posed by state-supported foreign entities — such as BGI and MGI — in the U.S. biotech sector. The task force would issue regular legislative and regulatory recommendations to safeguard sensitive research and supply chains.

- **Strengthen federal procurement restrictions**: Through measures like the BIOSECURE Act, prohibit U.S. federal agencies from purchasing BGI and MGI sequencers, ensuring no federal funds support entities linked to the CCP.

- **Amend Federal Grant Guidelines to Prohibit High-Risk Partnerships**: Bar federally funded research partnerships with Chinese biotech firms like BGI and MGI in sensitive fields, allowing exemptions only under strict oversight and transparency requirements to prevent unauthorized data transfers or infiltration.

Cameras and Surveillance Systems

- **Ban DHS Procurement of Cameras from High-Risk Vendors**: Prohibit DHS and its sub-agencies from purchasing or deploying surveillance cameras produced by entities linked to Chinese state or military organizations, ensuring that no federal dollars support compromised systems.

- **Mandate Comprehensive Risk Assessments**: Require federal and critical infrastructure operators to conduct periodic security evaluations of installed camera systems —

especially those from Chinese manufacturers — identifying remote-access vulnerabilities or hidden firmware backdoors.

- **Add Major Chinese Surveillance Firms to the 1260H List**: Request DHS coordination with the Department of Defense and other agencies to include key Chinese camera manufacturers, such as Tiandy, on the Chinese Military-Industrial Companies list, restricting their access to U.S. capital markets and federal procurement.

- **Sanction Firms Facilitating Human Rights Abuses**: Enforce targeted sanctions against Chinese companies that provide surveillance technology enabling human rights abuses, blocking them from U.S. financial systems and dissuading others from similar collaborations.

Conclusion

By enacting robust supply chain oversight, technology-specific restrictions, and rigorous investment screening, the House Homeland Security Committee can decisively blunt Beijing's infiltration, prepositioning, and profiteering. Each recommendation falls squarely within the Committee's legislative and oversight purview. By moving from a reactive stance to a proactive defense, Congress will safeguard U.S. critical infrastructure, deny Xi Jinping the leverage he seeks, and ensure that America's homeland security remains resilient in the face of China's aggressive techno-strategic ambitions.