United States House Committee on Homeland Security

March 5, 2025

Threats from PRC Cyber Actors and Transnational Criminal Groups for the hearing on "Countering Threats Posed by the Chinese Communist Party to U.S. National Security"

Testimony by **Dr. Rush Doshi**
Assistant Professor of Security Studies, Georgetown University Walsh School of Foreign Service
C.V. Starr Senior Fellow for Asia Studies and Director of the China Strategy Initiative, Council on Foreign Relations

---

Chairman Green, Ranking Member Thompson, distinguished members of the Committee, thank you very much for the opportunity to testify at today's hearing.

I will focus my remarks on some of the challenges China poses to homeland security:

1. First, what are Beijing's ambitions?
2. Second, how does it threaten homeland security in the cyber domain?
3. Third, how does it threaten homeland security through transnational crime?

I. PRC Ambitions and Intentions

The Chinese Communist Party is a nationalist political party dedicated to the goal of national rejuvenation after what it perceives as a "century of humiliation" at the hands of imperial powers. Related to that objective, the PRC has a grand strategy to displace U.S.-led order.[1] It seeks to "catch up and surpass" the U.S. technologically; to make the world dependent on China's supply chains economically; and to acquire the capability to defeat U.S. forces militarily.

The PRC is a capable rival too. It is the leading industrial power with more than 30% of all global manufacturing.[2] It is pursuing military bases around the world and in the Western hemisphere. It is also the first U.S. competitor to surpass 70% of U.S. GDP in a century.[3]

The PRC's preferred alternative for global order would be substantially different from the U.S.-led order that has prevailed since the end of the Cold War. It is discernable in speeches by senior PRC leaders. Politically, Beijing would project leadership over global governance and international institutions, split Western alliances, and advance autocratic norms at the

expense of liberal ones. Economically, it would weaken the financial advantages that underwrite U.S. hegemony and seize the commanding heights of the "fourth industrial revolution" from artificial intelligence to quantum computing, with the United States declining into a "deindustrialized, English-speaking version of a Latin American republic, specializing in commodities, real estate, tourism, and perhaps transnational tax evasion."[4] Militarily, the People's Liberation Army (PLA) would field a world-class force with bases around the world that could defend China's interests in most regions and even in new domains like space, the poles, and the deep sea. The fact that aspects of this vision are visible in high-level speeches is strong evidence that China's ambitions are not limited to Taiwan or to dominating the Indo-Pacific.

The PRC perceives the international system as providing opportunity for the PRC to achieve national rejuvenation. Since 2017, Xi has in many of the country's critical foreign policy addresses declared that the world is in the midst of "great changes unseen in a century" [百年未有之大变局]. The phrase captures the idea that the order is once again at stake because of unprecedented geopolitical and technological shifts, and that this requires strategic adjustment. For Xi, the origin of these shifts is China's growing power and what it saw as the West's apparent self-destruction. On June 23, 2016, the United Kingdom voted to leave the European Union. Then, a little more than three months later, a populist surge catapulted Donald Trump into office as president of the United States. From China's perspective—which is highly sensitive to changes in its perceptions of American power and threat—these two events were shocking. Beijing believed that the world's most powerful democracies were withdrawing from the international order they had helped erect abroad and were struggling to govern themselves at home. The West's subsequent response to the coronavirus pandemic in 2020, and then the storming of the U.S. Capitol by extremists in 2021, reinforced a sense that "time and momentum are on our side," as Xi Jinping put it shortly after those events.[5] China's leadership and foreign policy elite declared that a "period of historical opportunity" [历史机遇期] had emerged to expand the country's strategic focus from Asia to the wider globe and its governance systems.

Although the PRC poses a variety of challenges to the United States, this testimony focuses on two in particular relevant to this jurisdiction and that affect millions of Americans: (1) the threat posed by PRC cyber actors, particularly to U.S. critical infrastructure, and (2) the threat posed by PRC criminal actors, especially in production and money laundering related to Fentanyl.

We now turn to each respectively.

II. PRC Cyber Threats to Personal Data, Intellectual Property, Government Systems, and Critical Infrastructure

PRC cyber actors have compromised sensitive U.S. networks with multiple objectives.

First, the PRC seeks access to American personal data for intelligence purposes. In the last decade, the PRC has hacked the Office of Personnel Management, Equifax, Mariott, Anthem Health Insurance, and multiple airlines – compromising hundreds of millions of records.[6]

Second, the PRC seeks access to American intellectual property. The PRC has infiltrated American companies to steal what some estimate at over $1 trillion of U.S. intellectual property.[7] PRC cyber actors have compromised cloud providers that handle data for hundreds of companies.[8]

Third, the PRC seeks access to government systems. In the last two years, PRC actors compromised tens of thousands of emails from the State Department, Treasury Department, and other agencies. Notably, the PRC targeted Microsoft Exchange Online, which allowed it to compromise 60,000 State Department emails and compromising the account of U.S. Commerce Secretary Gina Raimondo, U.S. Ambassador to China Nicholas Burns, and others. It is still unknown how the PRC was able to do this, and the incursion was first detected by the State Department.

Fourth, and most concerning, the PRC is preparing the operational environment for wartime using cyber instruments. Government officials and private sector leaders have increasingly called attention to PRC activity in U.S. critical infrastructure that could pose a direct threat to homeland security. Earlier this year, CISA, NSA, FBI, and Five Eyes partners assessed that, "that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States," and that a PRC group called "Volt Typhoon" had comprised infrastructure providers in several sectors.[9] At the Munich Security Conference a few weeks later, Deputy National Security Adviser Anne Neuberger explained further that, "For a long time when we all in the industry talked about cyber security our key focus was theft of data...what has shifted as captured in the Volt Typhoon threat vector is countries pre-positioning in the critical infrastructure of another country." Neuberger explained that "we know it is not for espionage purposes, because when we look at the sectors like water sectors and civilian airport sectors, those have very little intelligence value." She continued, "That is a concern because a potential disruption of critical infrastructure could be used to put pressure on a government during a crisis or could be used to put pressure or try to message to a population during a crisis.[10] As Jen Easterly said to the Select Committee on the CCP, the PRC is ready to "launch destructive cyber-attacks in the event of a major crisis or conflict with the United States," including "the disruption of our gas pipelines; the pollution of our water facilities; the severing of our

telecommunications; the crippling of our transportation systems." These steps would be designed to "to incite chaos and panic across our country and deter our ability to marshal military might and citizen will."[11]

The private sector is aware of the problem. As Microsoft CEO Brad Smith explained, "we've seen from China in particular this prepositioning of so-called web shells. Think of it as tunnels into our water system, our electrical grid, into the air traffic control system, the kind of thing that you look at and you say, this is only useful for one thing and that's they have it in place in the event of a war or hostilities."[12] In an annual report last year, Microsoft noted it had been tracking some of the relevant threat actors focused on U.S. critical infrastructure for several years.

In general, the United States needs to shrink its attack surface while investing in offensive operations against the PRC to establish deterrence.

First, Congress should prohibit software companies that sell to the U.S. government from operating in China. Several U.S. technology companies that serve the U.S. government have provided the PRC government the source code of the systems that the U.S. government and most Americans rely on. In 2003, Microsoft allowed China to participate in its Government Security Program which it indicated "provides national governments with controlled access to Microsoft Windows source code."[13] More recently, in 2016, Microsoft launched a "Transparency Center" in China to provide "access to documents and source code" for "Windows, Windows Server, Office, Exchange Server, SQL Server, and SharePoint Server," services upon which the U.S. government also depends.[14] Similarly, in 2015 IBM decided to allow the Chinese government review its source code in a controlled environment.[15]

Second, Congress should prohibit cloud operators that support the U.S. government from operating in China. These companies almost certainly face conflicts given the PRC's regulatory environment. The PRC has introduced a National Intelligence Law, Counterespionage Law, Encryption Law, Data Security Law, and updates to its definition of state secrets in recent years. This regime gives the PRC the ability to demand PRC entities and individuals comply with requests from the intelligence services, provide access to encryption keys, insert personnel on site, or outright seize equipment and data. In that regime, the fact that U.S. cloud operators in China are required by the Chinese government to partner with a Chinese operator is concerning. Microsoft, for example, partners with 21 Vianet, to operate Microsoft's cloud services in China, including Azure; Amazon partners with Beijing Sinnet Technology Co., Ltd. (Sinnet) and Amazon Web Services Ningxia Region run by Ningxia Western Cloud Data Technology, Co., Ltd. (NWCD). Others, like Google and Oracle, do not offer services in China.[16] For those that do, the concern is whether their systems in China are adequately firewalled from systems in the United States, or whether compromise of cloud infrastructure in China could be used to compromise U.S. systems. Even with such firewalls, it is conceivable that PRC operating partners could gain important

insights into how their U.S. partners provide cloud services to clients in the United States, important information about network topology and architecture. More fundamentally, the fact that PRC operators may be operating a PRC cloud with encryption keys provided to the PRC government all under a regime that gives broad authority to PRC intelligence services to embed themselves in the operator suggests data stored in U.S. cloud systems in the PRC is not secure.

There are reasons to believe the PRC is focused on gaining advantages from these kinds of entanglements. For example, technology companies supporting the U.S. government may be forced to cooperate with China's cybersecurity legislation by providing information on zero-days that the PRC government appears to be promptly weaponizing. Microsoft has publicly accused the PRC of using the country's new vulnerability disclosure requirements to stockpile zero-day exploits. "China's vulnerability reporting regulation went into effect September 2021," it wrote in a 2022 report, "marking a first in the world for a government to require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared with the product or service owner." Based on the data, Microsoft concludes that, "the increased use of zero days over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority."[17]

What is particularly concerning is the possibility that the PRC may be learning more about systems on which the U.S. relies while reducing its own reliance on U.S. systems. Conversely, we may not be able to gain comparable information about PRC systems. Over time, this creates a structural asymmetric vulnerability. This is not a purely academic consideration. For example, even as Microsoft was increasing PRC visibility into its products, the PRC was reducing its reliance on Microsoft products and forcing public service providers and others to switch to the indigenous PRC HarmonyOS system. During the recent outage related to a CrowdStrike update, PRC public services – in contrast to U.S. services – experienced "minimal impact." PRC government employees boasted that this "proved that the country has made progress in achieving its goal of 'safe and controllable' computing systems." Accordingly, there are risks that the information shared with the PRC about U.S. technology systems could create asymmetric vulnerabilities. Similarly, although U.S. cloud providers do have some market share in China, they are small compared to Chinese cloud providers who have successfully increased their market share. As with consulting, the benefits from involvement in the PRC marketplace are likely falling while the risks are growing. As Microsoft CEO Brad Smith noted in recent testimony, China accounts for about 1.5% of Microsoft's revenue and is scaling down its engineering team. At the same time, the PRC is backing its own cloud providers in foreign markets, and the opportunity for U.S. providers in the market is shrinking while the risks continue to grow.[18]

Third, Congress should codify the Information Communication Technology and Services Supply Chain Executive Order and fund the office that administers it. This lets us prohibit certain PRC goods that connect to networks. The Biden Administration used this Trump-era tool keep out PRC connected vehicles. But that's just the start. Recently, DHS CISA has found backdoors in PRC-made medical devices.[19] The time for action is now.

Finally, the United States needs to go on the offensive. If the PRC has accesses on U.S. critical infrastructure, the United States reciprocally needs to maintain access on PRC critical infrastructure. That will take resourcing and staff. Presently, the PRC has invested in that kind of manpower, but the United States generally has not. Accordingly, this Committee's Cyber PIVOTT Act can help boost our workforce for defense and offense.[20] Related to all of this are better defensive measures. Notably, the United States needs common sense regulation of the private sector, which right now has little incentive to upgrade its cybersecurity.

III. PRC Transnational Criminal Activity, Fentanyl, and Money Laundering

Two-hundred Americans die every day due to Fentanyl overdoses.[21] According to the DEA, Fentanyl overdoses are the leading cause of death for Americans between 18 and 45 and are responsible for 70% of overdose deaths in the United States.[22] In 2020, the DEA released a report on the flow of Fentanyl which found that, "China remains the primary source of Fentanyl and Fentanyl-related substances trafficked through international mail and express consignment operations environment, as well as the main source for all Fentanyl-related substances trafficked into the United States."[23] The PRC is directly complicit in the flow of Fentanyl to the United States.

The PRC gives tax rebates and grants to Chinese chemical companies for manufacturing and exporting Fentanyl precursors.[24] The PRC not only provides state-sponsored support to these companies; the Select Committee on the CCP found that the party holds direct ownership interest in at least four companies with connections to illicit drug sales.[25] The PRC also allows these companies to advertise their goods openly on PRC websites.[26] Moreover, PRC underground banks help cartels launder Fentanyl profits. These banks take hard dollars from the cartels in America and provide them pesos in Mexico; they then sell those dollars to Chinese citizens who want their cash out of China and take renminbi in China as compensation.[27] These transactions do not require the actual flow of funds across borders.

The PRC has taken steps to address this issue only twice: in 2019 and more significantly in 2023, when they went after some companies, shut down websites, took down advertisements, went after some money launderers.[28] But these actions are still inadequate. Ultimately, the PRC has the power to stop the precursor flow. They can stop money laundering too, which occurs on apps like WeChat that the PRC government monitors for dissidents. But for now, the PRC has not done so. Beijing instead appears to prefer to keep the issue alive for leverage with Washington.

As for possible solutions, Congress needs to strengthen U.S. sanctions authorities against entities involved in the Fentanyl trade, including PRC financial institutions.[29] Relatedly, Congress can also link progress on Fentanyl to other PRC priorities, in consultation with the administration. To combat money laundering, Congress should pass the Corporate Transparency Act so law enforcement can track the beneficial owner of PRC shell companies and crack down on money laundering.[30] Finally, Congress should pass the HALT Fentanyl Act to place Fentanyl-related substances as a class into schedule I of the Controlled Substances Act.[31] By imposing stricter penalties on Fentanyl, the law could deter international trafficking from China and strengthen law enforcement efforts against international drug trafficking networks.

I'll end with this. The PRC poses many challenges to homeland security. The issues addressed in this testimony affect the lives of tens of millions of Americans. The China challenge is abstract, so it is important we link it to the lives of everyday Americans.

With that I thank you for your time and look forward to your questions.

---

[1] Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (Oxford University Press, 2021).

[2] Dave Evans, "China's Crossroads: Challenges & Opportunities For The World's Factory," *Forbes*, November 26, 2024, https://www.forbes.com/sites/daveevans/2024/11/26/chinas-crossroads-challenges--opportunities-for-the-worlds-factory/; China Power Team, "Measuring China's Manufacturing Might," China Power, Center for Strategic and International Studies, last updated December 18, 2024, https://chinapower.csis.org/tracker/china-manufacturing/.

[3] Micah McCartney, "How China's Economy Compares to the US's After Latest Results," *Newsweek*, July 16, 2024, https://www.newsweek.com/china-us-economies-compared-1925603.

[4] Michael Lind, "The China Question," *Tablet*, May 19, 2020, https://www.tabletmag.com/sections/news/articles/china-strategy-trade-lind.

[5] Xi Jinping [习近平], "Xi Jinping Delivered an Important Speech at the Opening Ceremony of the Seminar on Learning and Implementing the Spirit of the Fifth Plenary Session of the 19th Central Committee of the Party" [习近平在省部级主要领导干部学习贯彻党的十九届五中全会精神专题研讨班开班式上发表重要讲话], Xinhua [新华], January 11, 2021.

[6] "Cyber Operations Tracker," Council on Foreign Relations, https://www.cfr.org/cyber-operations/. See also, Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/; Katie Benner, "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking," *New York Times*, February 10, 2020, https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html; David E. Sanger, Nicole Perlroth, Glenn Thrush, and Alan Rappeport, "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *New York Times*, December 11, 2018, https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[7] Estimates vary, but all align around roughly at least $1 trillion in losses is conservative. See, Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report*, February 27, 2017, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf; Nicole Sganga, "Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies," *CBS News*, May 4, 2022,

https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/.

[8] Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's failed fight against China's 'Cloud Hopper' hackers," *Reuters*, June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

[9] United States of America, Australian Government, Dominion of Canada, United Kingdom of Great Britain and Northern Ireland, New Zealand, *Joint Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity & Infrastructure Security Agency (US), National Security Agency (US), Department of Justice (US), Department of Energy (US), Environmental Protection Agency (US), Transportation Security Administration (US), Signals Directorate (AUS), Cyber Security Centre (AUS), Communications Security Establishment (CAN), Centre for Cyber Security (CAN), National Cyber Security Centre (NZ), National Cyber Security Centre (UK), AA24-038A, February 7, 2024, https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.

[10] Anne Neuberger, "MCSC 2024: Fireside Chat: Anne Neuberger," Sicherheitsnetzwerk München, March 11, 2024, YouTube video, https://www.youtube.com/watch?v=WlvcT3aPb2k.

[11] Jen Easterly, "Opening Statement by CISA Director Jen Easterly," Blog, News, Cybersecurity& Infrastructure Security Agency, January 31, 2024, https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly.

[12] *A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security*, 118th Congress, 2nd session, 2024, (Statement of Brad Smith, Vice Chairman and President, Microsoft).

[13] "Microsoft and China Announce Government Security Program Agreement," Stories, Microsoft, February 28, 2003, https://news.microsoft.com/2003/02/28/microsoft-and-china-announce-government-security-program-agreement/; "China Information Technology Security Certification Center Source Code Review Lab Opened," Stories, Microsoft, September 26, 2003, https://news.microsoft.com/2003/09/26/china-information-technology-security-certification-center-source-code-review-lab-opened/; "Microsoft Gives Chinese Government Access to Windows Source Code," *People's Daily*, March 4, 2003, http://en.people.cn/200303/04/eng20030304_112657.shtml.

[14] Laramillermsft and MicrosoftGuyJFlo, "Transparency Centers," Articles, Microsoft Security, Microsoft, February 2, 2024, https://learn.microsoft.com/en-us/security/engineering/contenttransparencycenters.

[15] Eva Dou, "IBM Allows Chinese Government to Review Source Code," *Wall Street Journal*, October 16, 2015, https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

[16] "Cloud Locations," Google, https://cloud.google.com/about/locations#asia-pacific; Public Cloud Region Locations, Oracle, https://www.oracle.com/cloud/public-cloud-regions/.

[17] Microsoft, *Microsoft Digital Defense Report*, Security Insider, Microsoft, 2022, 39-40, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[18] Mark Montgomery and Eric Sayers, "Don't Let China Take Over the Cloud — US National Security Depends On It," *Hill*, November 13, 2023, https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/.

[19] "Contec CMS8000 Contains a Backdoor | CISA," February 13, 2025, https://www.cisa.gov/resources-tools/resources/contec-cms8000-contains-backdoor.

[20] "Chairman Green Reintroduces 'Cyber PIVOTT Act,' Senator Rounds to Lead Companion Legislation – Committee on Homeland Security," February 5, 2025, https://homeland.house.gov/2025/02/05/chairman-green-reintroduces-cyber-pivott-act-senator-rounds-to-lead-companion-legislation/.

[21] USAFacts Team, "Are fentanyl overdose deaths rising in the US?" *USAFacts*, last updated September 27, 2023, https://usafacts.org/articles/are-fentanyl-overdose-deaths-rising-in-the-us/.

[22] "DEA Administrator on Record Fentanyl Overdose Deaths | Get Smart About Drugs," accessed March 3, 2025, https://www.getsmartaboutdrugs.gov/media/dea-administrator-record-fentanyl-overdose-deaths.
[23] "Fentanyl Flow to the United States," Drug Enforcement Agency Intelligence Report, DEA-DCT-DIR-008-20 (2020), https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf.
[24] "Select Committee Unveils Findings into CCP's Role in American Fentanyl Epidemic," April 16, 2024, https://selectcommitteeontheccp.house.gov/media/reports/select-committee-investigates-ccps-role-fentanyl-crisis
[25] Ibid.
[26] Ibid.
[27] Joe Miller and James Kynge, "The New Money Laundering Network Fuelling the Fentanyl Crisis," *Financial Times*, June 27, 2024, https://www.ft.com/content/acaf6a57-4c3b-4f1c-89c4-c70d683a6619.
[28] Alex Willemyns, "Rubio Accuses China Of 'Reverse' Opium War Via Fentanyl," *Radio Free Asia*, February 27, 2025, https://www.rfa.org/english/china/2025/02/27/china-rubio-fentanyl-opium-war/.
[29] Congress.gov. "H.R.10447 - 118th Congress (2023-2024): CCP Fentanyl Sanctions Act." December 17, 2024. https://www.congress.gov/bill/118th-congress/house-bill/10447.
[30] Congress.gov. "H.R.2513 - 116th Congress (2019-2020): Corporate Transparency Act of 2019." October 23, 2019. https://www.congress.gov/bill/116th-congress/house-bill/2513.
[31] "Grassley, Cassidy, Heinrich Propose Permanent Scheduling Fix for Fentanyl-Related Substances | United States Senate Committee on the Judiciary," January 30, 2025, https://www.judiciary.senate.gov/press/rep/releases/grassley-cassidy-heinrich-propose-permanent-scheduling-fix-for-fentanyl-related-substances.

STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE HOUSE HOMELAND SECURITY COMMITTEE

AT A HEARING REGARDING "COUNTERING THREATS POSED BY THE CHINESE COMMUNIST PARTY TO THE U.S. NATIONAL SECURITY"

MARCH 5, 2025

Chairman Green, Ranking Member Thompson, and members of the Committee — it's an honor to appear before you today.

I have spent 32 years working in the U.S. Government, twenty-four of which as a Special Agent with the FBI, and as Chief of Counterespionage at the CIA.

I was tremendously honored to serve as the first Senate confirmed Director of the National Counterintelligence and Security Center (NCSC) in May 2020, leading our nation's Counterintelligence and security efforts. I served in that role since 2014.

I am here before you today as the CEO of The Evanina Group, LLC. In this role, I work closely with CEOs, Boards of Directors, and academic institutions, and senior executives of the U.S. Government to provide a strategic approach to mitigating corporate risk in a complicated global environment.

A DOMESTIC THREAT LANDSCAPE OVEVIEW

EXISTENTIAL THREAT

Our nation continues to face an array of diverse, complex, sophisticated, and unprecedented threats by nation state actors, cyber criminals, and terrorist organizations.

Unquestionably, the existential threat our nation emanates from the Communist Party of China (CCP). This comprehensive threat posed by the CCP is the most complex, pernicious, strategic, and aggressive threat our nation has ever faced. It is an existential threat to every fabric of our great nation. Now, more than ever, the private sector and academia have become the modern battlefield for which Xi's holistic efforts manifest.

Xi Jinping has one overarching goal to be the geopolitical, military, and economic leader in the world. Xi, along with China's Ministry of State Security (MSS), People's Liberation Army (PLA), and the United Front Work Department (UFWD), drive a comprehensive and whole of country approach to their efforts to invest, leverage, infiltrate, influence, and steal from every corner of the U.S. This is a generational battle for Xi and China's Communist Party (CCP), it drives their every decision.

REAL COSTS OF ECONOMIC LOSS

The estimated economic loss from the theft of intellectual property and trade secrets, just from the CCP, and just from known and identified efforts, is estimated between $300 Billion and $600 Billion per year (Office of the U.S. Trade Representative and Federal Bureau of Investigation).

To make it personal for you and your constituents, this theft equates to approximately $4,000 to $6,000 per year, per American family of four…after taxes.

China's ability to holistically obtain our intellectual property and trade secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed. Actually, it is said by many to be the largest theft of intellectual property in the history of the world….and it has happened just in the past decade.

Additionally, it is estimated that 80% of American adults have had all of their personal data stolen by the CCP, and the other 20 percent has had most of their personal data stolen. For Xi, the overarching vison is how to counter, compete, and push past the U.S. is goal number one.

TERRORISM REDEFINED

Congress, and the entire American democratic and capitalistic ecosystems, must first clearly understand Xi's reprehensible intentions in order to effectively mitigate the accompanying threat with our own whole-of-society approach.

We must approach this existential threat with the same sense of urgency, spending, and strategy, as we have done for the past twenty-four years in preventing terrorism in our homeland.

To set the perspective, a simple definition of terrorism is "the use of threats or violence to achieve political or ideological goals."

I would offer to this committee that we are in a terrorism event. A slow, methodical, strategic, persistent, and enduring event which requires an increased degree of urgency of both government and corporate action. It is clear that under

Xi Jinping, the CCP's economic war with the U.S. has manifested itself into a clear terrorism type of framework.

Let me be more specific. The CCP's capabilities and intent are second to none as an adversary. Cyber breaches, insider threats, surveillance and penetrations into our critical infrastructure have all been widely reported. Adding in the CCP's crippling stranglehold on so many aspects of our supply chain and the result is a montage of domestic vulnerability of unacceptable proportions.

Recent nefarious and disturbing areas of the CCP's actions include VOLT and SALT TYPHOON, surveillance balloons, technical surveillance stations in Cuba, maritime cranes, Huawei, TikTok, strategic land purchases near military and strategic locations, influence at the state and local level, etc. When overlapped, the collage begins to paint a bleak mosaic which is beyond the blinking red metaphor. It is imperative to understand that the CCP maintains civil unrest and societal chaos as a primary pillar in any nefarious cyber penetration or attack.

EVERYTHING EVERYWHERE ALL AT ONCE

I would ask this committee: Is it not terrorism when our electrical grid or a natural gas pipeline is disabled via VOLT TYPHOON in a part of the U.S., resulting in millions of households, schools, hospitals, and buildings being without heat or electricity? What about when our telecommunications infrastructure (e.g., Verizon, AT&T, and T-Mobile) being disabled on the same day due an organized cyber-attack, precipitated by SALT TYPHOON? And if our financial services sector was impacted and had to go offline, for even a few hours, it would cause significant domestic and international chaos, societal panic, and disruption.

Are these not terror type events? If these events coincidently occur as the CCP makes their inevitable move on Taiwan, will the American people, and U.S. policy makers for that matter, have the sufficient appetite to actually defend Taiwan?

The CCP has strategically planned and implemented the ability to do just this, all at once, and all across our homeland. Hence, "terror" must be redefined beyond our framework which historically includes loved ones being injured or killed from a kinetic event.

The inability or unwillingness to look behind the curtain and visualize this clear and realistic scenario is no longer an option for anyone, especially the Congress, the Administration, U.S. governmental entities, academic institutions, and especially the private sector. In fact, the proverbial curtain to look behind no longer exists. We must immediately end the process of being victims to the CCP's actions.

SALT TYPHOON

The largest telecommunications hack, in the world, occurred in 2024. It occurred here, in the U.S., by CCP backed hackers, against the top nine U.S. based telecommunications carriers and hardware providers. The size and scope of this brazen hack has not yet been determined and will take extensive time to do so. This successful hack by the CCP provided comprehensive call and text data of subscribers, geolocation of the subscribers, and ability to listen to telephone conversations as they deemed interested. Per public reporting, the intent of the breach was to obtain court ordered warrant data issued to the carriers by the U.S. Government on Chinese targets. Similar to the OPM breach, the CCP succeeded beyond their dreams and intentions. It is much worse than that, but that is for a closed session with your U.S. Government agencies.

As an intelligence and law enforcement professional, I am beyond concerned with this access for all the obvious intelligence and counterintelligence gathering aspects. Additionally, the thought that a foreign adversary and competitor can access metadata call information and listen to conversations, is beyond astonishing, and very disheartening. As members of this Committee are fully aware, for this to happen here, legally in the U.S., a FISA or Title 3 court order, signed by a U.S. Magistrate Judge or FISA Court would be required.

FENTANYL

Let us take a look at the fentanyl epidemic. Members of this Committee are very familiar with the epidemic and the numbers. But it is important to revisit and place into comparison perspective. Thankfully we have recently seen a significant reduction in deaths caused by fentanyl overdoses. However, with over 200 Americans dying of fentanyl overdose every day (107k+ in'23), China's effect is analogous to a Boeing 737 aircraft crashing, every day, and killing everyone on board. The fentanyl epidemic is delivering the same casualty rate within the U.S. as Germany and Japan delivered to American soldiers in World War II. Currently, fentanyl overdoses per day are 50% greater than the World War I Killed-in-Action per day count. Let that sink in. And as members of this committee are already aware, most of the fentanyl precursors are manufactured in China. The fentanyl epidemic starts, and ends, with the CCP.

MARITIME PORTS

Specific adversaries (Russia/China) have been historically creative in embedding intelligence collection capabilities into products which have a legitimate use in business, commerce, technology, or operating systems (see Kaspersky Labs). The CCP has taken this concept to increasingly strategic, and potentially paralyzing levels.

The new frontier, in my opinion, is the legitimate procurement by U.S. port terminals of Chinese manufactured (Shanghai Shenhua Heavy Industries Company, Limited) ZPMC crane systems.

ZPMC is a subsidiary of China Communications Construction Company (CCCC). CCCC is a prominent contractor for the Peoples Liberation Army and Navy. Members of the Committee are aware that it is currently estimated that approximately 80% of all of the ship-to-shore goods and services entering, and exiting, the U.S. are offloaded/loaded via Chinese owned ZPMC crane systems. Additionally, these same ZPMC crane systems are used by the U.S. military to commission our Naval and Coast Guard vessels at numerous strategic ports.

ZPMC cranes offer the CCP a dual use capability for intelligence collection (cameras, sensors, tracking technology, connected software) in U.S. ports servicing heavy commercial activity as well as U.S. military bases. The ZPMC crane systems provide a supply chain vulnerability of potentially paralyzing proportions. There is interconnectivity among all the ZPMC crane systems nationwide, and shared Chinese developed software and labor. ZPMC, if ordered by the CCP, can immediately shut down maritime port operations throughout the U.S. in a time of conflict or to utilize a future economic lever.

Additionally, other elements of the product transportation supply chain are also required to enter into these contracts, including data sharing agreements, and software collaboration while working at a U.S. maritime port ecosystem in order to interface with ZPMC cranes and technology.

When the ZPMC crane system threat is stacked onto the VOLT TYPHOON cyber malware penetration, the CCP will be able to systematically, and without delay, cause instant havoc in almost every aspect of American daily operations, commerce, and safety, and at the same time instill a level of societal and business panic not seen since September 1, 2001.

In my professional opinion, and from a civilian and military perspective, this might be the CCP's most strategic operational endeavor against the U.S. thus far, outdistancing Huawei. We cannot allow it to be their most successful.

INSIDER THREAT

The Insider Threat problem, originating from the CCP, has been nothing short of devastating to the U.S. corporate world, academic institutions, and research and development organizations in the past decade, plus. The Department of Justice's web site's catalog of economic espionage indictments and convictions is staggering. The result is hard to swallow and quantify. And those listed cases only represent what was identified, reported by a U.S. company, and then prosecuted.

We need to continually highlight this issue as a key facilitator for the CCP's strategic endeavors to steal intellectual property and trade secrets, especially those developed before they are classified by the U.S. Government, as well as the CCP's strategic placement for human enabled cyber operations.

Corporate America and academia must make significant efforts to identify and mitigate insider threats to their organizations seeking to steal and/or do harm. It starts with a more substantive vetting process of applicants and incorporation of an insider threat or employee wellness program. It is too costly not to. The impacts ripple far beyond the victim company.

HOW DOES THE THREAT MANIFEST?

Intelligence services, joint ventures, science and technology investments, academic collaboration, research partnerships, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions, initiate the comprehensive and strategic framework for how China implements their strategy.

China continues to successfully utilize "non-traditional" collectors to conduct a plurality of their nefarious efforts here in the U.S. due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, IT professionals, and students, are shrouded in legitimate work and research. Oftentimes, the "non-traditional" collector becomes an unwitting tool for the CCP and its intelligence collection apparatus.

China's ability to holistically obtain our Intellectual Property (IP) and Trade Secrets via illegal, legal, and sophisticated hybrid methods is beyond demoralizing. Joint ventures, creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes and similar programs on university campuses, talent recruitment programs, investments in emerging technologies, and utilization of front companies, continue to be the framework for strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre-and-post patent application.

ACADEMIA A LEADING TARGET

The threat posed by China to U.S academia, as well as research institutions (including federal), is deep, pervasive, and decades long. The past decade of indictments and prosecutions have highlighted the insidiousness of China's approach to obtaining early and advanced scientific research and data.

Additionally, China has expertly learned and manipulated the complexity and shrouding of gifts and funding at U.S. colleges and universities, particularly when tied to federal grants. On-going academic partnerships by U.S. universities with CCP cultural programs (Confucius Institutes) and CCP funded research institutions is increasingly problematic, and one-sided.

For example, the University of Michigan, and other universities, recently severed ties with China's Shanghai Jiao Tong University (SJTU). SJTU has historically been tied to the CCP's intelligence and cyber hacking programs. The University of Michigan's brave and bold decision was only possible after the university was provided briefings, intelligence, and data as to the nefarious history and activities of SJTU by this Congress, and the FBI.

Universities need to be sufficiently advised of ongoing threats and risk in order to make sound risk-based decisions on said partnerships. Additionally, universities who continue to engage in these CCP partnerships with known nefarious activities need to be held accountable for such relationships.

There is a clear void in this problem set which requires immediate fixing. The U.S. Government, specifically the FBI, NSA, DHS, and others, must be forward leaning in dissemination of known threat intelligence to academia and research institutions. Such effort is critical to enable immediate and strategic risk-based mitigation decisions to protect not only ideation and trusted development of intellectual property, but also individual university brands.

This is increasingly important as we are in a high-speed technology race with China and cannot afford for China's continuance of easy theft and hence, not earning their place in this critical twenty-first century competition for technology dominance. I address this further in my recommendations.

ACADEMIC DUE DILIGENCE AND COMPLIANCE

U.S. academic and research institutes must engage in rigorous due diligence and compliance programs. I spend a considerable amount of business with academic institutions advising and informing them on due diligence and compliance efforts to identify and mitigate potential areas of concern with foreign students, professors, and researchers. Recently, an executive of a very prestigious U.S. university stated: "I assumed the Department of State vetted these students

prior to coming on campus. What do you want us to do?" This assumption, and related question, is very common and very problematic.

The U.S. possesses the greatest catalog of academic and research institutions and entities the world has ever seen. The U.S. continues to not only be the leaders in the world, but with such, we attract the best and brightest from around the world. The collaborative nature of academia is primary to its success; however, it is also its greatest vulnerability.

Vetting of foreign national students, faculty and research, if it occurs, is nascent at best, and in just a few institutions. The dilemma and complexity I hear from institutions is understandable. However, we can no longer continue to allow the CCP to obtain the ideation, hard work, research, and patent ready results, from U.S. academic and research institutions without any effort to defend such.

This situation is also similar to U.S. government entities such as the National Institute of Health, National Science Foundation, Department of Energy, National Labs, and so many others. To ensure security of our hard work and related product, compliance and due diligence must be a priority if we have any chance at slowing down the CCP from obtaining classified, and unclassified, research with minimal difficulty.

INDUSTRIES LEADING AS TARGETS

China's key priorities for obtaining U.S. based technology and know-how, pursuant to their publicly available "Made in China 25 Plan" are Aerospace, Deep Sea Technology, Biotechnology, Information Technology, Advanced Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics.

Any CEO or Board of Directors engaged in any of these critical industries, and within the vertical supply chain, must understand the threat posed to them and work to identify risk-based mitigation strategies. This is a zero-sum game.

"Military-Civil Fusion" is undoubtably a strategy employed by the CCP to drive Xi's movement to global technological and military dominance. However, it is too often viewed through a western based filter and related bias. In China, there is no fusion of military and civilian efforts. They are ONE, working together, and in unison. Unlike the U.S. and other western-based democratic nations, there does not exist a bifurcation between government, military, and the private sector. I would even include the education ecosystem in this mosaic. There is one China. Xi's China. Everything, and everyone, works toward a common goal in China, which is the betterment of China.

Additionally, the People's Liberation Army (PLA) and Ministry of State Security (MSS) have never been so collaboratively intertwined with respect to common goals and aggressiveness of action as they have been the past five to ten

years. If the PLA needs a specific technology for military capability to copy or reverse engineer, the MSS will acquire it through any means necessary and will employ every legal, and illegal, tool as referenced earlier, in obtaining the necessary technology.

CHINA DOES NOT PLAY BY ANY RULES

China plays by their own rules, only. China does not conform to any international or normalized set of regulations, guidelines, norms, laws or value-based agreements throughout the global economic ecosystem.

To further the CCP's unlevel economic playing field, out of the 15 largest companies inside China, 13 are either owned by the CCP, or run by the CCP. The world has seen recently what the CCP is capable of when one of the largest companies in the world, Alibaba, pushes back on state-run efforts. Additionally, many of the CCP's largest corporate leaders and CEO's have gone missing.

Boards of Directors and investment leaders must begin to think strategically about what the long-term threat impact the CCP presents and how their investments, decisions, and unawareness of the long-term threat impact their respective businesses and industries. This threat is woven with our national security, economic stability, and endurance of our republic. As a nation, and if we truly want to compete with China, we must move toward a more intertwined risk-based intelligence sharing effort between the U.S. government, corporate America, and academic institutions.

CHINA'S NEED TO KNOW LAWS

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere, and in any way. Three specific portions of these laws should be understood, and be an enduring reminder to CEOs, General Counsels, Chief Data Officers, CIOs, CSOs and CISOs, throughout our private sector ecosystems.

The first is Article 7 of the People's Republic of China National Intelligence Law summarily stating that all business and citizens *shall* cooperate with China's intelligence services and shall protect all national work secrets.

The second is Article 77 of the same National Security Law summarily stating that Chinese citizens and business *shall* provide anything required or requested by the Chinese government or intelligence services.

The third is Article 28 of the 2016 Cybersecurity Law summarily stating that all network operators *must* provide data to, and anything requested by, national, military or public security authorities.

These laws carry with every Chinese citizen whether they reside in Beijing, or anywhere else in the world, regardless of their employer. Hence, a Chinese National working at a U.S. company is always at risk for answering to the CCP's data collection apparatus.

YOUR DATA IS CHINA'S DATA

As a cautionary tale, if you are a U.S. business seeking to enter a business relationship with a company in, or from, China, your data will be obtained and provided to the MSS or PLA for their usage, without exception. This includes any third-party data as well. The analogy is a U.S.-based company entered into a business deal or partnership with a company from another country. In order to do business, the U.S. company would be required to provide all relevant and requested data from their company, as well as the partner company, to their customer agency, such as the NSA, CIA and FBI. To reiterate, the operational and legal tempo of the CCP is difficult to visualize and understand while looking through western and democratic lenses. There is no bifurcation between the CCP and corporate ecosystem. It is one China.

MALIGN INFLUENCE

Malign foreign influence has increased dramatically in the U.S. in the past decade. Russia, China, and others have been very active in this activity and with varying degrees of success. Measuring such activity has proven to be not a perfect science.

China is strategic and precise as they successfully influence at the state and local levels of the U.S. I want to briefly touch on a few key areas.

The first is economic investment. Chinese investments in key industries such as real estate, agriculture, advanced manufacturing, and technology have raised significant concerns. These partnerships often take the form of "Sister City Programs but can also be business partnerships between a city or small town and a CCP owned or controlled company. Investments in U.S. critical infrastructure at the local level is also on the rise which creates an entire separate category of concern.

The CCP takes advantage of small towns and cities increasing need for economic solicitation of funds. CCP partnerships with Economic Development professionals provides the most immediate and impactful results. The town, or city, receive immediate investment and the CCP obtains a foothold, access, or future opportunity for strategic purposes. Local Economic Development professionals have no idea of the ultimate purpose or intent of such a partnership.

Political donations and lobbying are another serious concern. The CCP's strategic approach to identify current, and future, political leaders and elected officials and invest in their future continues to be problematic. The investment can take form in direct financial support to a campaign, lobbying, or placing CCP loyalists into the inner circle of an elected official to influence decision making to benefit CCP interests or individuals supporting CCP efforts.

The most common initial step is the official invite of a newly elected federal, state, or local official for an all-expense paid trip to China with family and friends where the CCP will offer investments and inexpensive solutions to the elected official's economic challenges. As well, the CCP will gain access to the elected official's mobile devices.

The obvious and immediate need is to have a platform where state and local (and even federal) elected officials can receive substantive training and awareness of how these issues manifest in their state, city or township.

THE NEED FOR STRATEGIC LEADERSHIP

In closing, I would like to thank this Committee for acknowledging the significant threat posed by China by holding this hearing. Continuing to drive awareness, and more importantly, combat the threat posed by the CCP will take a whole-of-nation approach with a mutual fund type long-term commitment. Such an approach must start with robust and contextual awareness campaigns, like this Committee holding this hearing. The WHY matters.

Regarding these awareness campaigns, we must be specific and reach a broad audience, from state and local governments to academia, from board rooms to business schools, educating on how China's actions impair our competition by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders.

Our nation needs strategic leadership now more than ever, particularly when we face such an existential threat from a capable competitor who is looking beyond competition to global dominance. We have to catch up, mitigate and inflict costs on China in an expedited fashion. Doing such will entail strategic leadership leading a whole-of-society approach is imperative.

Lastly, I would like to state for the record the significant national security threat we face from the Communist Party of China is NOT a threat posed by Chinese people, as individuals. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and will stop at nothing to achieve his goals. As a nation, we must put the same effort into this threat as we did for the terrorism threat. The threat from China, particularly with respect to the long-term existential threat is hard to see and feel, but I would

suggest it is as dangerous, if not more dangerous, than terrorism to our viability as a nation.

RECOMMENDATIONS:

The holistic and existential threat posed by the CCP is one of the few bipartisan areas of agreement in the U.S. Congress today. We must, as a nation, compete at the highest level possible while at the same time understand the gravity and urgency, and what is at stake.

Below are some recommendations:

1. Implement an aggressive real time and actionable threat sharing by the U.S. Government with private sector. **Create an Economic Threat Intelligence entity which delivers actionable, real-time threat information** to CEOs, Boards of Directors, state and local economic councils to enable risk-based decision making on investments and partnerships. This intelligence delivery mechanism should include the Intelligence Community, FBI, Department of Commerce, Department of Treasury, and CISA. The core constituency should be state and local entities at risk and utilize existing vehicles such National Governors Association and the Chamber of Commerce to increase threat awareness of illicit activities investment risk at the state and local level.

2. Congress must ensure U.S. government agencies are leaning aggressively forward in providing collected intelligence to corporate America pertaining to plans and intentions, as well as nation state activities, in software, coding, supply chain and zero-day capabilities. **The U.S. Government must be more effective in providing intelligence expeditiously to the private sector.** Enhanced declassification of collected intelligence (especially in the technology arena) with respect to threats to our economic well-being, industries, and companies must be delivered at speed to impacted entities prior to the threat becoming realized.

3. **Maintain bipartisan congressionally led public hearings** to advise and inform CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors of the threat posed by the CCP, and how they are targeted.

4. **Create a panel of CEOs who can advise and inform Congress and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private sector supply chain dilemmas.** I would recommend a *Business Round Table* type of framework. Membership should be diverse and include but not be limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity and Venture Capital. This entity should be co-chaired by a CEO from the above group.

5. **Establish an over-the-horizon panel to discuss, in a public forum, emerging technology which may potentially pose a long-term threat (AI/ML, Quantum, Aerospace) to the long-term economic well-being of America.** The first topic should take a close look at the strategic investments the CCP is making into state and local pension plans, CCP's strategic land purchases, Sovereign Funds, as well as foreign investment into the Federal Thrift Savings Plan and other state/local retirements vehicles.

6. **Reestablish the National Security Higher Education Advisory Board (NSHEAB).** This board should have 25 college and university Presidents as members with a Chair and Co-Chair and be housed and facilitated by the Federal Bureau of Investigation in partnership with the CIA and NSA. All members will be provided security clearances at the Top-Secret level in order to be provided real time threat and awareness information the U.S. Government possess to help guide academia in risk-based decisions and partners. This entity existed until the FBI closed the program in 2014.

7. **Create a National Training Center for elected officials.** This center will provide baseline training to newly elected officials and their staff on what malign influence looks like (examples of recent situations) and how to best mitigate such efforts. Additionally, what will surely occur on your first trip to China as an elected official, particularly with your mobile devices.

8. **Create a platform where each Governor of the U.S. can establish his/her own CIFIUS-Lite program to identify and mitigate nefarious economic investments and land purchases within their respective states.** This framework will provide intel and data sharing from the Treasury Department's CIFIUS Program, the FBI, DHS, and other law enforcement and intelligence entities to assist individual U.S. states on what to look, how such nefarious activity manifests at the local level, and how to most effectively mitigate.

   Again, I am honored to be here today and thank the Committee for holding this hearing to better understand and mitigate the existential risk posed the CCP to our national security.

Testimony Before the House Committee on Homeland Security on "Countering Threats Posed by the Chinese Communist Party to U.S. National Security." Wednesday, March 5, 2025. 310 Cannon House Office Building.
Michael Pillsbury (The Heritage Foundation)

Good morning Chairman Green, Ranking Member Thompson, and members of the Committee on Homeland Security.

Thank you for the opportunity to be one of your witnesses to comment on the subject of dealing with the China threat to U.S. national security.

I am a fan of this committee's work on China. One vivid example is your February report on the committee website titled "China Threat Snapshot," which provides voters with a detailed description of Chinese espionage in the last three years.[1] The revelation of these details will sicken American patriots. Another example: The committee has been rightly skeptical about the *2025 Annual Homeland Security Threat Assessment*, raising questions about how China is described. I would hope that the authors within the department's 800-person Intelligence and Analysis unit are doing something more about China than the report seems to indicate.

My first recommendation today is that the committee provide focus by developing a list of specific initiatives on China to win the much-discussed strategic competition. There are some good ideas in Senator Tom Cotton's new national number one bestseller, *Seven Things You Can't Say About China*. I would recommend that everyone buy this short book of 30,000 words. I can't resist revealing the seventh point he makes: "China May Win." Now, as Chairman of the Senate Intelligence Committee, Senator Cotton describes a world in which China will "supplant" America as the dominant superpower.[2] This is an important concept that I'll return to. Our new CIA Director, John Ratcliffe, has also committed at his confirmation hearing to focus on the greatest threat: China. In this context, what exactly can the Committee on Homeland Security do? What is its comparative advantage among other committees and with respect to the executive branch?

Today, there is no shortage of ideas about how to deal with the threat from China. The problem is these ideas are often not relevant, filled with loopholes, or may never be implemented. The challenge we face is that ten years of complacency may stretch into ten more years. I served as a co-editor of one of the Heritage Foundation's special reports, *Winning the New Cold War: A Plan*

[1] House Committee on Homeland Representative Subcommittee on Counterterrorism and Intelligence, "China Threat Snapshot," https://homeland.house.gov/wp-content/uploads/2025/02/CCP-Threat-UPDATED-Feb-2025.pdf
[2] Tom Cotton, *Seven Things You Can't Say About China* (New York: Broadside Books, 2025), 154

for Countering China.[3] We assembled as many legislative ideas as we could find to deal with the China threat. We found more than eighty and broke them down into four categories in our publication. Many of the ideas were proposed by single sponsors and a few co-sponsors, but didn't make it past committee.

China is watching this American inactivity. During my visits to China since my 2015 book, *The Hundred-Year Marathon*, was published, Chinese officials and scholars have pointed out how weak the American Congress has been in dealing with the China threat. Chinese think tanks and professors keep careful track of our China policy. A common Chinese view is that efforts by America's Congress to counter China have been vague and often watered down to mere rhetorical flourishes. Still other legislative proposals just disappeared in conference. Remember that Communist China's experts on American politics usually have American university degrees and read our press carefully. We lack equivalent coverage of China's politics, in part due to massive Chinese secrecy about issues we care the most about.

When I ask Chinese experts on America to score who is ahead, the answer is always "China."

In 2000, the National Defense University published my book on how the Chinese government scores power among nations using complex quantitative formulas. To my surprise, the Chinese translated that book and it was sold in China as *China Debates the Future Security Environment*.[4] I revealed estimates by the PLA and other government sources that China would be equal or surpass America by around 2020—not in terms of GDP, but based on a more complex scoring system called Comprehensive National Power, or CNP. Soon after, China stopped making these forecasts public, although Xi Jinping himself often refers to the concept of CNP.

My recommendation is that we need to score our competition with China like any other game or match, just like how we count football touchdowns. But first, we need to decide what to cover.

The Heritage Foundation's *Winning the New Cold War* did not evaluate through an index of indicators the extent to which we are succeeding or failing in the Marathon against China. My speculative scoring (over the last two years since it was published) of the eighty legislative initiatives it assembled would be China: 80, America: 0. We would do better if we had concrete indicators showing what we should accomplish over the long term. This would enable legislative initiatives to turn into tangible outcomes which would give us what President Trump called "leverage" in his 2015 book.[5] Frankly, we might have to go beyond legislative initiatives,

---

[3] Heritage Foundation, "Winning the New Cold War: A Plan for Countering China," https://www.heritage.org/sites/default/files/2023-07/SR270.pdf. See executive summary, 5-15. See also the final chapter by Michael Pillsbury, "The Way Forward," 116-118.

[4] Michael Pillsbury, *China Debates the Future Security Environment* (Washington: National Defense University Press, 2000), https://nuke.fas.org/guide/china/doctrine/pills2/index.html

[5] Donald Trump, *Great Again: How to Fix Our Crippled America* (New York: Threshold Editions, 2015), 45

embracing ideas like committee letters to the President or cabinet secretaries or a congressional committee visit to Beijing to convey seriousness and learn the source of Chinese arrogance stemming from their rise, as Xi Jinping repeats in speeches.

Why is this happening? The Heritage Foundation's special report, *Winning the New Cold War*, has highlighted that one source of China's success has been its successful lobbying by unregistered agents supported by the CCP who exploit a loophole in the Foreign Agents Registration Act.[6] In the past few weeks, the U.S. Attorney General, Pam Bondi, has been seeking comments on tighter control of Americans acting as agents for China, but the public commentary to Justice seeks to block these crucial improvements. You can see for yourself by going to the DOJ website to read the debate.[7] Foundations and universities who want to be rewarded for their pro-China advocacy fear the shame they would suffer if they had to register publicly as "foreign agents." If the online replies to Bondi's effort are any guide, Chinese lobbying operations inside our country will have free rein. After all, the criminal penalty for failure to register is five years in prison for each count.

Last month marked the ten-year anniversary of the publication of my book, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower*. In 2015, despite clear indications to the contrary, Washington was only just coming to the realization that China represents an existential, geopolitical threat to the United States. The book thus outlined twelve steps at the end that American policymakers would need to follow to compete in the so-called Marathon against China, the long-term race to the position of global superpower that we find ourselves in today.

Ten years after my attempt to alert Washington to the urgency of the 100-year Marathon, we have made almost no progress. It might be fruitful for me to walk through each of my twelve steps—which are even more pertinent today—to pinpoint the path that we need to follow in order to make up for our delayed start in the Marathon.

I must note the parallel recommendations offered in another best-selling book that appeared ten years ago called *Great Again: How to Fix Crippled America*. As I alluded to earlier, the author was President Donald J. Trump. Mr. Trump asserted correctly that there are two different kinds of Chinas: a good China that built great cities and provided housing and education for millions of people, and a "bad China," the one that "is the one mostly hidden to outsiders."[8] Its government controls internet access, engages in political repression, stifles free expression, arrests dissidents, restricts individual freedoms, and launches cyberattacks.

---

[6] Heritage Foundation, "Winning the New Cold War," 7

[7] "Amending and Clarifying Foreign Agents Registration Act Regulations," *Federal Register*, January 2, 2025, https://www.federalregister.gov/documents/2025/01/02/2024-30871/amending-and-clarifying-foreign-agents-registration-act-regulations#

[8] Trump, *Great Again*, 42

Mr Trump was one of the first to identify the long-term China threat to our country. His stark conclusion in 2015 was the same as mine: We've been losing the battle to China for a long time. Trump warned that our economies are tied together in a very negative way. In his assessment, he used the exact same word as I did: "replace," writing that "economists have made predictions that within the next decade, China will replace the United States as the world's largest economy."[9] Then, he raised the subject of this hearing today: "What have we done to beat them?" His answer was "I'll tell you what we've done. We've rolled over."[10] They have "destroyed entire industries by utilizing low wage workers, cost us tens of thousands of jobs, spied on our businesses, stolen our technology, and have manipulated and devalued their currency, which makes selling our goods more expensive - and sometimes, impossible."[11]

Mr Trump and I had parallel recommendations about the idea of leverage. Trump asked, "So what should we do about it? We're going to use the leverage we have to change the situation so that it favors America and our people. I've negotiated with Chinese companies. I know how they do business."[12]

Mr. Trump's diagnosis was more poignant than my book. He created a sentence I wish I had written which is still valid today: "When dealing with China we need to stand up to them and remind them that it's bad business to take advantage of your best customer."[13] In words that sound like they were only spoken yesterday, Trump wrote, "We should sit down and figure out how to make this a more equitable relationship."[14]

Let's turn to my twelve recommendations, which remind us that we have been addicted to China and that we need to end our dependence and instead use our leverage, as Mr. Trump advised, to get back on track.

The first step I proposed then was the most basic one, and fortunately, perhaps the one where we can say that we have made some limited progress: recognizing that China is a competitor. Even if we have come to a general recognition, there are still strikingly some voices on both sides of the political aisle that hold out naive hopes about Beijing's future. Just recently, Senate Minority Leader Chuck Schumer—who has expressed great concern over Trump's China tariffs[15]— was spotted posing for photos with CCP officials who have spread CCP propaganda and denied

---

[9] Trump, *Great Again*, 43
[10] Trump, *Great Again*, 43
[11] Trump, *Great Again*, 43
[12] Trump, *Great Again*, 45
[13] Trump, *Great Again*, 47
[14] Trump, *Great Again*, 47
[15] Kevin Scott, "Schumer Melts Down Over Trump's China Tariffs," *Knewz*, February 24, 2025, https://www.msn.com/en-us/news/politics/schumer-melts-down-over-trump-s-china-tariffs/ss-AA1zDkGj?ocid=BingHPCNews

allegations about the mistreatment of Uyghurs in China.[16] Although it is frequently repeated in Washington that China presents an existential threat to the U.S.' geopolitical predominance, words do not equate to actions. Key politicians on both sides of the political aisle are hesitant to take decisive action that would harm their relationship with the CCP.

The second step that I proposed in my book was for Congress to enact an annual reporting requirement of all the assistance flowing from American agencies and departments to China. This has still not happened at a broad, congressional level. Various agencies have taken it upon themselves to verify whether they are directly or indirectly benefiting China. The Department of Defense's annual reports on military and security developments relating to China[17] and the Commerce Department's tracking of whether key technologies are being transferred to China[18] are two examples. But these agency-specific directives fall short of documenting the total financial assistance flowing from American coffers to the Chinese government.

The same pattern repeats itself for my third step. I had suggested that the White House "provide Congress with an annual report that includes trends and forecasts about how the United States is faring relative to its chief rivals."[19] There is still no single, consolidated report that does this, but just like the assistance reporting, some agencies are partially fulfilling this requirement. The ODNI's Annual Threat Assessment, the White House's periodic National Security Strategies, and the U.S.-China Economic and Security Review Commission Annual Report are three examples of initiatives that are already underway that could be combined into a single, comprehensive report measuring U.S. competitiveness vis-à-vis China.

This ties in to the next recommendation which I included in the book, which was for the U.S. to create a competitiveness strategy. Again, we have made significant progress in terms of acknowledging the military, political, technological, and economic threat posed by China in our key defense and intelligence reports, but we are lacking multi-agency documents—somewhat like the IC's National Intelligence Estimate—which regularly outline a strategy for competitiveness that we should follow to beat China in the Marathon. We don't quite know what the finish line is, which makes it hard for us to determine what we are competing for. If this were well articulated in a coherent strategy, it would save a lot of time and dissonance between federal agencies all adopting their own unique strategies.

---

[16] Andrew Mark Miller , Cameron Cawthorne, "Schumer spotted posing for photo with CCP official as warnings swirl about China influence," *Fox News*, February 19, 2025, https://www.foxnews.com/politics/schumer-spotted-posing-photo-ccp-official-warnings-swirl-china-influence

[17] U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2024," https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

[18] U.S. Department of Congress, "U.S. Trade with China," 2022, https://www.bis.doc.gov/index.php/country-papers/3268-2022-statistical-analysis-of-u-s-trade-with-china/file

[19] Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company, 2015), 217

The fifth step which I proposed was to find common ground at home. There is admittedly a more broad consensus today compared to 2015 that China represents a critical threat to the U.S.-led world order. That being said, as just mentioned, we are missing a grand strategy as to *how* we should approach this threat. Nancy Pelosi's 2022 Taiwan visit and the subsequent backlash which this triggered was an example of an American failure in this regard. This episode signaled that we have two divergent China strategies—one provocative and the other conciliatory—which we cannot agree on.[20] In our competitiveness strategy, we need to get both parties and people from private companies, civil society, and government united behind a single approach as to how we should approach China in the decades to come.

The sixth step I had proposed is one where we are not doing as poorly. I had argued for the necessity of building a vertical coalition of nations. There has been some laudable bipartisanship in terms of U.S. rapprochement to our Asian allies. The U.S. has spearheaded trilateral cooperation with Japan and Korea, both administrations have reinforced our contributions to the Quad, both have supported the Philippines in the face of Chinese bellicosity in the South China Sea, and our bilateral talks with Indian Prime Minister Narendra Modi have been regular and productive.[21] Secretary of State Marco Rubio's decision to exempt Taiwan and the Philippines from the recent foreign aid freeze demonstrates the Trump administration's willingness to reinforce its coalition of Asian allies to encircle China.[22]

In my seventh step, I had noted our obligation to shine a light on China's political dissidents pushing back against the authoritarian system from which they have fled. I criticized the Obama Administration for not including human rights in the 2009 Strategic and Economic Dialogue. Once again, we have failed to be on the side of dissidents exposing China's humanitarian crimes. Admittedly, Trump's two administrations took a tough stance against China with regards to the Uyghurs. Former Secretary of State Mike Pompeo systematically highlighted the religious persecution happening in China, which drew responses from human rights organizations in the United States and inspired a series of legislative efforts from several U.S. federal agencies.[23] Current Secretary of State Marco Rubio recently condemned Thailand for sending Uyghurs back to China.[24] Since then, however, most of that progress has grinded to a halt because of how much Beijing has tightened its security apparatus. The U.S. will have to continue funding outlets which

---

[20] Isaac Chotiner, "The Provocative Politics of Nancy Pelosi's Trip to Taiwan," *The New Yorker*, August 4, 2022, https://www.newyorker.com/news/q-and-a/the-provocative-politics-of-nancy-pelosis-trip-to-taiwan
[21] Derek Grossman, "The State—and Fate—of America's Indo-Pacific Alliances," *RAND*, November 1, 2024, https://www.rand.org/pubs/commentary/2024/11/the-state-and-fate-of-americas-indo-pacific-alliances.html
[22] Jimmy Quinn, "Rubio Exempts Taiwan and Philippines Security Programs from Aid Freeze," *National Review*, February 23, 2025, https://www.nationalreview.com/corner/rubio-exempts-taiwan-and-philippines-security-programs-from-aid-freeze/
[23] United States Holocaust Museum, "US Responses to China's Crimes Against the Uyghurs," https://www.ushmm.org/genocide-prevention/countries/china/us-responses-to-chinas-crimes-against-the-uyghurs
[24] Michael Martina and David Brunnstrom, "US condemns Thailand's return of 40 Uyghurs to China," *Reuters*, "https://www.reuters.com/world/asia-pacific/us-condemns-thailands-return-40-uyghurs-china-2025-02-27/

give dissidents the ability to criticize the regime from afar. This will be discussed more further in my remarks.

The eighth step in the 100-Year *Marathon* is one that has dominated headlines in the past decade, and often not for the right reason: stemming Beijing's anti-American competitive conduct. The U.S. has still failed to decouple its military supply chain production from China.[25] Chinese cyberespionage has recently targeted American telecommunications[26] and NATO military systems.[27] Chinese hackers have targeted intellectual property to match the pace of American research—which has become especially concerning as of late in the AI sphere.[28] There is a constant tension between transparency and geopolitical competitiveness in the American system: We have a tendency to make our models open source and to reveal more than we should about the details of our military programs, which allows competitors to replicate our strengths. One need only look at the plagiarism in Chinese military aircraft and ships.[29] Since there is an obligation for Chinese citizens abroad to report back to the CCP, states will have to tighten their security to prevent CCP-controlled firms from collecting information on American citizens, buying farmland, and infiltrating American military infrastructure. Arkansas Governor Sarah Huckabee just recently took a stand against this by introducing new legislation to curtail the ability for CCP-operated firms to operate in her state—a move in the right direction.[30]

My ninth step leads us to the topic of pollution. At the time, I had suggested that American public officials emphasize China's failure to uphold climate agreements and unacceptable pollution levels. It is more difficult to make this argument today with regards to electric vehicles, since Beijing strives to have 40 percent of the vehicles sold at home be EVs by 2030.[31] China has also determined that it is in its own interest to refine its early warning systems and launch ozone pollution reduction programs by the end of 2025 to address the smog and air contamination problem it has been facing for several decades.[32] Whether or not it will succeed in this goal

---

[25] Dan Nidess, "Face the facts: America has outsourced its military supply chain to China." *The Hill*, January 17, 2025, https://thehill.com/opinion/5090860-us-china-trade-war-impact/
[26] Amir Daftari, "Major Chinese Cyber Espionage Targeting US Telecom Networks Uncovered by FBI," *Newsweek*, November 14, 2024, https://www.newsweek.com/fbi-chinese-cyber-espionage-multiple-telecom-networks-1985617
[27] Micah McCartney, "China's Spies Hacked NATO Allies Defenses, Official Says," *Newsweek*, February 8, 2024, https://www.newsweek.com/china-spies-hacked-nato-ally-netherlands-defenses-1868006
[28] House of Representatives Committee on Foreign Affairs, "Egregious Cases of Chinese Theft of American Intellectual Property," https://foreignaffairs.house.gov/wp-content/uploads/2020/02/Egregious-Cases-of-Chinese-Theft-of-American-Intellectual-Property.pdf
[29] Alex Hollings, "Counterfeit Air Power: Meet China's Copycat Air Force," *Popular Mechanics*, September 19, 2018, https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/
[30] Eric Shawn, "The plan to confront China and kick out companies controlled by the Chinese Communist Party from the U.S.," *Fox News*, February 26, 2025, https://www.foxnews.com/politics/plan-confront-china-kick-out-companies-controlled-chinese-communist-party-u-s
[31] Jennifer Conrad, "China is Racing to Electrify its Future," *WIRED*, June 29, 2022, https://www.wired.com/story/china-ev-infrastructure-charging/
[32] "China aims to eliminate severe air pollution this year," *Reuters*, February 25, 2025, https://www.reuters.com/business/environment/china-aims-eliminate-severe-air-pollution-this-year-2025-02-25/

remains to be seen. There seems, at least, to be some effort on China's side to reduce pollution and the harm it has done to the planet, though with self-interested goals in mind, of course. If anything is to be learned from the past few years, though, it is that if the United States slows down its industrial production for climate objectives, other countries like China will not necessarily follow suit. Climate agreements, from China's eyes, are only valid so long as they benefit Beijing's national security.

My tenth recommendation revolved around the fight against China's Great Firewall. I commended Wikipedia's battle against Chinese censorship, but encouraged the United States government to take the company's side and boost activity through Radio Free Asia. Unfortunately, there is little success to report in this regard. Last year, Radio Free Asia shut off all operations in Hong Kong due to fears that it would not comply with a security law.[33] This is understandable, since the families of Radio Free Asia journalists are often at risk, especially if they are of Uyghur descent.[34] But if Washington isn't able to penetrate the Great Firewall through outlets like Radio Free Asia, it should devise a concerted soft power or communications strategy that allows its information to infiltrate into Chinese society. Why is it that an application like TikTok has divided American society while no comparative American app like YouTube is able to convey information to Chinese people? Cracking the code of the Great Firewall will be one of the most pressing challenges for private companies assisting Washington.

Xi Jinping's authoritarian crackdown has made the eleventh step which I outlined excruciatingly difficult. I had suggested that the State Department fund more projects to promote the development of the rule of law and civil society in China. There has, of course, been no progress in this vein since Beijing strictly monitors State Department activities and the flow of money going to local initiatives and elected village officials. This should not prevent the American Embassy in Beijing from coordinating with Americans involved in the educational and private sector in China to provide support encouraging pro-democracy reform (or at least more separation from the CCP) to local institutions, however difficult that might be.

Finally, although Washington has recognized that China poses a threat to our global predominance—as stated at the start of my testimony—we still are dreadfully unfamiliar with the internal debates happening between the so-called 'hardliners' and 'reformers' in Chinese society. Since Xi runs the country in an authoritarian manner, we assume that China is a monolith, which disincentivizes us from having serious discussions in Washington about the disagreements that divide the CCP regarding China's future. The United States can only follow the strategies previously outlined—such as creating a competitiveness strategy—if we are aware of which faction within the CCP is prevailing at a given time. When the hawks are in power, we can

---

[33] David Pierson, "U.S.-Funded Broadcaster Leaves Hong Kong, Citing Security Law," *The New York Times*, March 29, 2024, https://www.nytimes.com/2024/03/29/world/asia/hong-kong-security-media.html
[34] Jay Nordlinger, "A Uyghur Daughter, and Journalist," *National Review*, May 4, 2021, https://www.nationalreview.com/2021/05/a-uyghur-daughter-and-journalist/

expect a more violent response from China every time we undertake some sort of rapprochement with our Asian allies or rid ourselves of Chinese technology in our military supply chains. Our strategy must be tailored to the internal dynamics within China, or else we risk missing opportunities to be more forward-leaning in our approach when reformers are more prominent in the CCP's leadership.

When we analyze the twelve steps that I proposed in the 100-Year *Marathon*, it becomes obvious that we have made little progress in the past decade. Yes, it is generally recognized in Washington that China is a threat, but that has translated to little concerted governmental action. Instead, the way it currently works is that each agency has mechanisms to verify whether the United States is funding China or how Chinese military and economic metrics have changed. There are few oversight methods that unite every agency and create clear indices pointing to whether we are beating China in the 100-Year Marathon. Now that 10 years have passed, it is about time to move from recognition to action, or else we risk being unable to recover from such a slow start.

EXCERPTS FROM THE 12 STEPS IN THE HUNDRED YEAR MARATHON

It's easy to win a race when you're the only one who knows it has begun. China is thus on its way to supplanting the United States as the global hegemon, creating a different world as a result. Yet it doesn't have to end this way.
.

STEP 1—RECOGNIZE THE PROBLEM

If America is going to compete in the Marathon, its thinking about China must change radically. This means recognizing that China is a competitor, not a welfare case.

STEP 2—KEEP TRACK OF YOUR GIFTS

Every year, a small fortune of American tax dollars is being spent to aid China's rise. Most of this aid is kept low-profile, unnoticed by the media and the public. This is done intentionally.

Labor Department experts who the U.S. government had sent to China to boost Chinese productivity….the Treasury Department and the comptroller of the currency offered China to improve its banking practices….the Federal Aviation Administration's assistance to Chinese aircraft manufacturers….other U.S. government agencies have facilitated hundreds of science assistance programs in China.

There is still no available accounting of all the activities funded by the U.S. government to aid China. Not only is America funding its own chief opponent; it doesn't even keep track of how much is being spent to do it.

To compete in the Marathon, Congress should enact an annual reporting requirement of all agencies and departments of their assistance to China. If such programs were identified and publicized, three beneficial results would follow.

STEP 3—MEASURE COMPETITIVENESS

Many of the Warring States stories involve carefully measuring the balance of power before strategies are chosen. It is a classic American business principle that "What you measure improves." The lesson is simple but profound: You can't improve unless you know what you need to improve. You can't come from behind in a race against your competitors unless you know the respects in which you have fallen behind. Every year, the Chinese create an annual analysis of their competitiveness relative to the United States. Why isn't America doing the same thing?

The U.S. government should be conducting a similar—but more robust— measure of American competitiveness. The White House should provide Congress with an annual report that includes trends and forecasts about how the United States is faring relative to its chief rivals. Many departments of the U.S. government, including the intelligence community, would have to be involved. It need not cover all other nations, just the top ten—beginning with China.

STEP 4—DEVELOP A COMPETITIVENESS STRATEGY

Stratagems of the Warring States frequently describes how leaders compete by adopting "reforms" to grow their power more rapidly than their competition. The point was to be open-minded enough to recognize and act when one's strategy needed to change, and then impose new tactics to achieve one's desired result.

The public policy analysts Robert Atkinson and Stephen Ezell have proposed a multiagency program to enhance American competitiveness, but they fear that it will be hampered or eliminated because of partisan political considerations.

STEP 5—FIND COMMON GROUND AT HOME

Warring States leaders tried to keep their allies closely aligned and built ever shifting coalitions united behind a common goal. Disunity was dangerous. There are many advocates for reforming American policy toward China—inside and outside of the U.S. government—but they are fractured into factions that often do not see each other as allies. Since at least 1995, Chinese scholars in Beijing have delighted in telling me stories of how Americans who criticize U.S. policy toward China are so divided by their political differences that they never cooperate.

STEP 6—BUILD A VERTICAL COALITION OF NATIONS

There is a reason why China has been expanding its South China Sea claims, bullying Philippine fishing boats, cutting the cables of Vietnamese seismic survey ships, and recently establishing an Air Defense Identification Zone in the East China Sea. China wants to guarantee access to a wealth of natural resources in the region and is hoping to intimidate its neighbors so they are too scared of China to unite and oppose its ambitions.

Whether you play wei qi or not, you know that encirclement by a group of adversaries is dangerous. China's natural fear is that its neighbors will form such an alliance. That's exactly what the United States should be encouraging with nations including Mongolia, South Korea, Japan, and the Philippines. Even the threat of such a coalition—through movements in that direction—might give Beijing pause and temper its bellicosity. China knows how America and its allies contained the Soviet Union. As the United States increases aid and facilitates cooperation among China's neighbors, China's hawks will get the blame when China feels isolated and alone in the region.

STEP 7—PROTECT THE POLITICAL DISSIDENTS

Many of the soldiers on the front line of the Cold War were Soviet and Eastern European dissidents who refused to surrender to an unending future of censorship, propaganda, religious persecution, and economic enslavement. Their field marshals were men such as Václav Havel, Lech Wałęsa, and Aleksandr Solzhenitsyn. And with their courage and passion and principles, they brought down the Soviet Union and the Iron Curtain. But they didn't do it alone. Presidents from Truman to Reagan championed their cause. When they were imprisoned, American presidents demanded their release. When they needed money, Americans sent them funds. When they needed a platform for the free speech their regimes denied them, Americans shared their printing presses and broadcast their battles and beliefs into millions of homes through Radio Free Europe.

Today China has increased its persecution of Buddhist Tibetans and Muslim Uighurs. In Tibet, the government has imposed curfews, arrested protesters, killed innocent civilians, and transformed the region into, in the recent words of the Dalai Lama, a "hell on earth." In Xinjiang, the Internet and phones are routinely shut off, and the percentage of Han Chinese in Tibet and Xinjiang has risen dramatically due to state-sponsored migration.

China also persecutes Christians. It is a common practice in China for foreigners to show their passports before being allowed to attend a church service in China. Why? Because China is ruled by the atheistic Communist Party, and its government wants to keep Chinese nationals out of non-state-run churches. Many experts estimate that there are 60 million to 100 million Christians in China and that the number is growing. Bob Fu, the founder and president of China Aid, seeks to equip the Chinese people to defend their faith and freedom. The organization's

purpose is to promote legal reforms, fund “house churches” in China, and assist imprisoned Christians.

STEP 8—STAND UP TO ANTI-AMERICAN COMPETITIVE CONDUCT

China is not just a source of cyber spying against the United States; it is the primary source. According to some estimates, more than 90 percent of cyber espionage incidents against America originate in China. 14 Chinese hackers regularly infiltrate American businesses and government entities. An abridged list of victims includes Google, Booz Allen Hamilton, AT&T, the U.S. Chamber of Commerce, Visa, MasterCard, and the Departments of Defense, State, Homeland Security, and Energy. Hacking is central to China’s decades-long campaign to steal technologies it can’t invent and intellectual property it can’t create. A report by the Commission on the Theft of American Intellectual Property, led by the former director of national intelligence Dennis Blair and by the former U.S. ambassador to China Jon Huntsman, found that the theft of U.S. intellectual property likely costs the American economy more than $300 billion per year. 15

STEP 9—IDENTIFY AND SHAME POLLUTERS

One of the more effective approaches to protecting the environment with regard to China occurred when Ambassador Huntsman authorized the U.S. embassy in Beijing to tweet the pollution levels in Beijing. 18 Similarly, Ma Jun the director of the Institute of Public and Environmental Affairs, a leading environmental watchdog organization in China, has compiled online maps of China’s water, air, and solid waste pollution.

But is fostering greater awareness the best we can do? The United States needs to go from asking China to act in an environmentally responsible way to insisting that China do so, even if that means using far more leverage than past administrations have been willing to exert. Otherwise, China will be at a competitive economic advantage—with Washington constraining American businesses in an effort to protect the environment while China goes right on exporting its products and its pollutants at breakneck speed.

STEP 10—EXPOSE CORRUPTION AND CENSORSHIP

One of the Chinese government’s greatest fears is of a free press. It knows that sunlight is a disinfectant for wrongdoing, and it is terrified of what its people would do if they knew the whole truth about Chinese leaders’ corruption, brutality, and history of lying about the United States and our democratic allies. Yet it remains a mystery why the United States doesn’t do more to fight China’s censorship and propaganda campaigns against the Chinese people.

But the government in Beijing uses its various tools to prohibit such information from reaching the Chinese people. In 2012 the Chinese government blocked Bloomberg News after it published a story on the family wealth of Xi Jinping. The implicit deal of working in China seems

to be this: you may report on China's fantastic growth, but if you start criticizing the Communist Party or its top officials you will be kicked out of the country.

During the Cold War, Radio Free Europe was an oasis for anti-Communist dissidents in a desert of Soviet censorship and propaganda. There's no reason why Radio Free Asia couldn't serve a similar purpose in the Hundred-Year Marathon, but its budget needs to be increased at least threefold.

STEP 11—SUPPORT PRO DEMOCRACY REFORMERS

China's concern when it talks about a new Cold War is that the Americans will revive their Cold War–era programs that helped to subvert the Soviet Union from within by using the power of ideas. Most Chinese hawks believe that this plan to subvert Chinese democracy has already been put into motion, much as it was for the Soviet Union in 1947. At least two Chinese books claim the CIA leads it.

Former secretary of defense Robert Gates has noted that the 1975 Helsinki Accords galvanized pro democracy groups inside the Soviet Union and played "a key role in our winning the Cold War." His view seems to be shared by the hawks of China, who write often about their fear that the United States has mounted a program to influence impressionable future civilian Chinese leaders to move toward democratic multiparty elections and a free market. 30 In October 2013, China's hawks revealed another fear—that America is seeking out a Chinese Gorbachev-like figure, a leader who will bring one-party rule to an end. The hawks' distrust of China's own leaders is shown in the tone of a ninety minute video released in October 2013 called Silent Contest. 31 China's hawks fear their civilian leaders are susceptible to influence from Western leaders who want to see multi party rule and an evolution toward democracy.

The truth is that there is no such concerted effort by the United States or the West to subvert China's Communist Party rule. The annual spending on programs to support democracy in China is less than $50 million. 33 While the U.S. government has some underfunded civil society programs, they are not CIA covert actions, and they are small in scale compared to what will be needed. There are at least six such programs, originating during the Cold War and run by various American organizations with U.S. government funds, including the AFL-CIO, the Chamber of Commerce, and both major U.S. political parties. They provide funding for a wide range of Chinese organizations inside China as well as for exile groups. 34

STEP 12—MONITOR AND INFLUENCE THE DEBATES BETWEEN CHINA'S HAWKS AND REFORMERS

Today, as China pursues its own Cold War strategy against America, it monitors carefully various factions in Washington, DC—those who are supporters of Beijing and those who are skeptics, those who can be manipulated and those who have caught on to the Marathon strategy. America used to be good at this, too. During the Cold War, the United States invested

time, technology, and personnel into discerning the activities among various members of the Soviet Politburo—those who advocated a more harmonious relationship with America and those who viewed the United States as a dangerous rival that must be overtaken. Yet unlike our activities against the Soviets, America is far behind when it comes to China.

It is crucial that the United States possess an understanding of the various actors in Beijing's sensitive internal debates. Though the Marathon strategy is moving apace, the Chinese government is not monolithic in its thinking. Hard- liners are certainly in the majority, but on the margins there are still sincere advocates of reform and liberalization who want a China that moves closer to an American-style model. They exist, and they must be identified and supported. The problem is that the U.S. intelligence community has not invested in the resources to determine who those true reformers are—as differentiated from the many Chinese leaders who make misleading reformist claims. This remains a massive intelligence challenge.

James Lilley, a former U.S. ambassador to China and a twenty-seven-year veteran of the CIA testified in August 2001, twelve years after the Tiananmen Square massacre, Lilley told a congressional commission that his greatest regret was learning a decade too late about internal Chinese documents revealing just how far China had moved toward democracy and how close the protests came to removing the Communist government. If only he had known at the time, the former ambassador said, he would have urged President George H. W. Bush to intervene firmly on the side of the real reformers, rather than being deceived by Beijing's leadership into siding with it.

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.

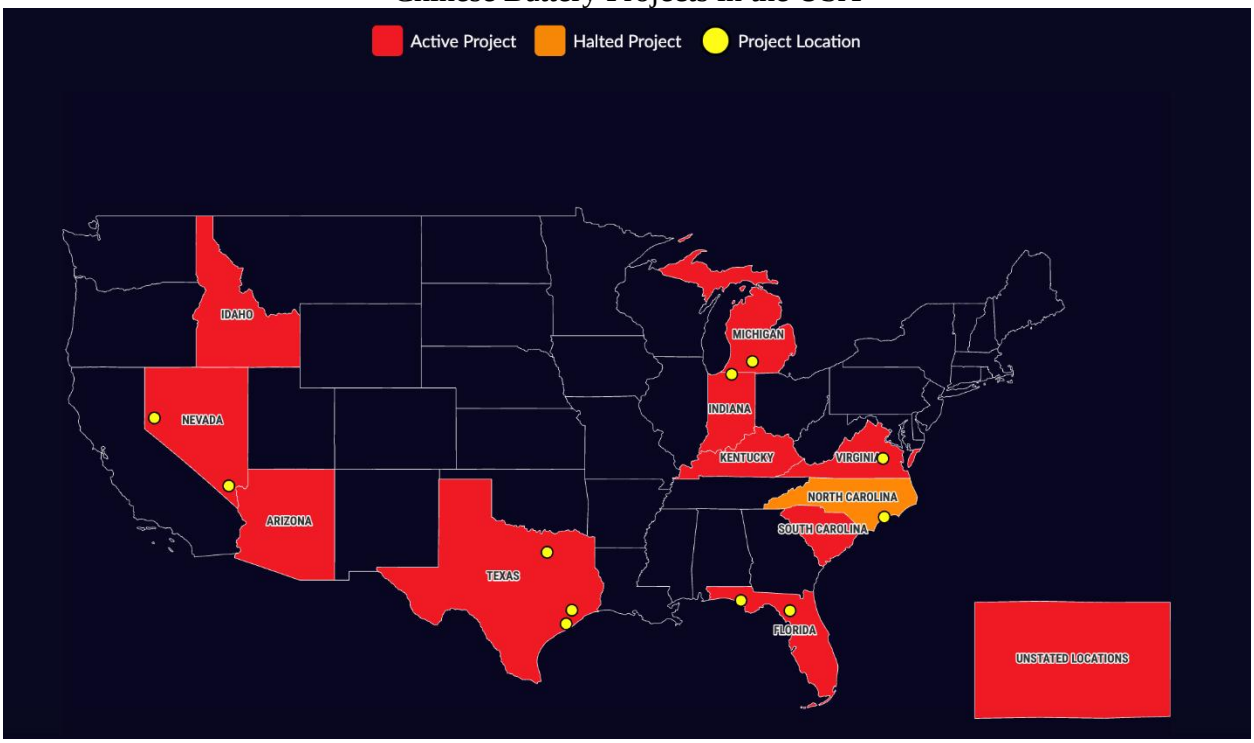
Leading Global Chinese Technology Firms

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.

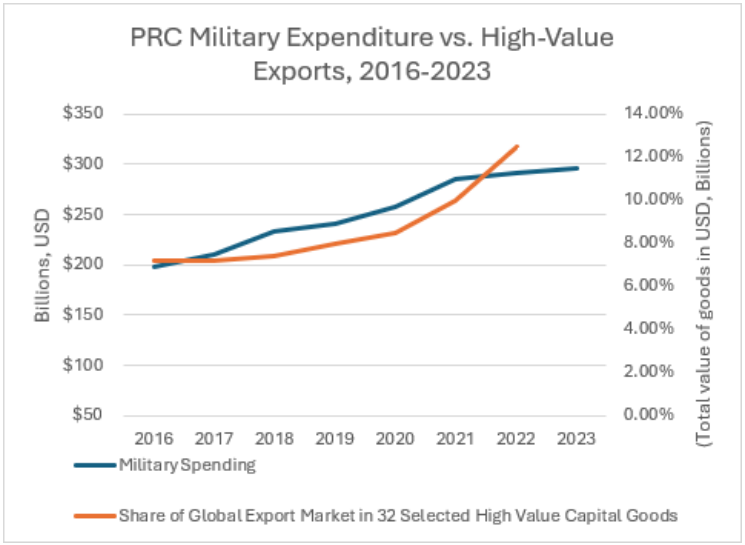
Ultimately, prepositioning is the logical outcome of Beijing's infiltration efforts; penetration itself is not the end goal but rather the vehicle through which China creates latent threats in both digital networks and physical supply chains. By embedding malicious capabilities — ranging from dormant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



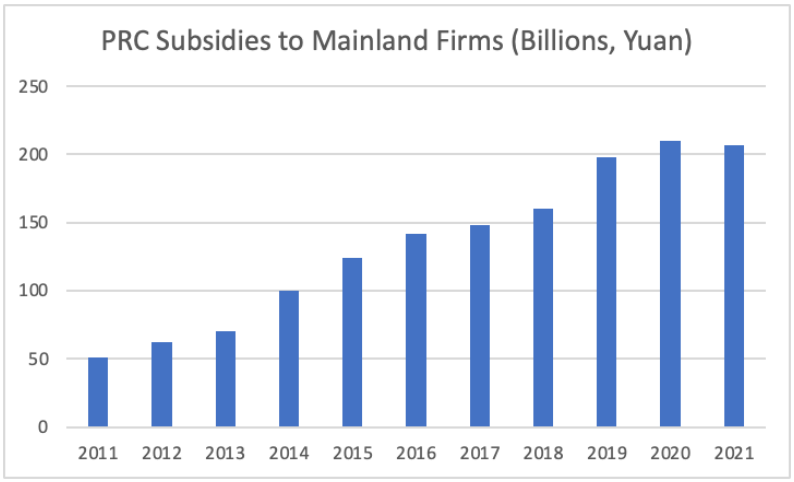
Source: Wall Street Journal; Statista; Department of Defense; Huawei; World Bank

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.