Statement before the House Homeland Security Subcommittee on Counterterrorism, Law Enforcement, and Intelligence

"Countering Threats from the CCP to the Homeland"

A Testimony by:

Kari A. Bingen

Director, Aerospace Security Project, CSIS

March 9, 2023

310 Cannon House Office Building

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss "Countering Threats from the CCP to the Homeland." The Center for Strategic and International Studies (CSIS) does not take policy positions, so the views represented in this testimony are my own and not those of my employer.

I have the privilege of leading the Aerospace Security Project at the Center for Strategic and International Studies, where I examine these issues largely through a national security lens, drawing from my experiences working at a U.S. technology startup, serving in the Department of Defense (DoD) guiding defense intelligence and security activities, and supporting the House Armed Services Committee.

Conflict with China is not inevitable, but the Chinese Communist Party (CCP) has been studying the United States, studying our way of war and our vulnerabilities, expanding and modernizing its military, using its economic influence to coerce others, and putting in place the pieces to "win without fighting." As stated in the Administration's 2022 National Security Strategy, the People's Republic of China (PRC) has ambitions "to become the world's leading power" and to "reshape the international order… to its benefit."[1] For the Department of Defense, the PRC is its "pacing challenge."[2]

Beijing has undertaken a broad campaign using all tools of national power and influence – diplomatic, economic, military, technological, and informational – to achieve its aims. While strategic competition and potential military conflict with China may seem abstract to many Americans, the Chinese surveillance balloon, shot down off the East Coast on February 4, 2023, was a tangible, visible signal that the U.S. homeland is not out of reach of Beijing's threats. It is also a reminder that the CCP's broad campaign for global power status and domination in the Indo-Pacific necessitates a focus on the U.S. homeland.[3]

I offer three areas where the CCP threat to the U.S. homeland is particularly acute: technology acquisition, critical infrastructure, and influence operations.

Technology Acquisition

Beijing has made it a national goal to acquire foreign technologies to advance its economy and modernize its military. It continues to comprehensively target advanced U.S. technologies, including in areas such as high-performance computing, biopharmaceuticals, robotics, energy, and aerospace. These are among ten areas that Beijing has explicitly identified

[1] "National Security Strategy," The White House, October 12, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[2] "National Defense Strategy of The United States of America," Department of Defense, October 27, 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.
[3] "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February, 7, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

as high priorities in its "Made in China 2025" strategic initiative to achieve technological superiority.[4] Aerospace is an example where Chinese President Xi Jinping has articulated his "space dream" to make China the foremost space power by 2045.

To acquire these technologies, Beijing uses both licit and illicit methods to target the people, information, businesses, and research institutions in the United States that underpin them. These methods include economic espionage, cyber data exfiltration, joint ventures, research partnerships, and talent recruitment programs, among others.[5]

The Director of National Intelligence's 2018 Worldwide Threat Assessment judged that, "most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or IT and communications firms."[6] Over the past several years, U.S. Department of Justice convictions or indictments highlight numerous of these methods in practice. Both Chinese nationals and U.S. citizens have been charged with economic espionage and attempted acquisition of sensitive U.S. defense technology in areas such as anti-submarine warfare, aviation, and submarine quieting technology.[7] Lucrative stipends, as part of Beijing's Thousand Talents Program, were offered to researchers to bring their technical knowledge to China.[8] Chinese real estate investors sought U.S. farmland and wind farms in proximity to U.S. military bases, and Chinese telecommunications equipment (e.g., Huawei devices) has been found near U.S. missile bases, all of which could be used to surveil or disrupt U.S. defense activities.[9]

---

[4] Karen M. Sutter, "'Made in China 2025' Industrial Policies: Issues for Congress," Congressional Research Service, December 22, 2022, 1, https://crsreports.congress.gov/product/pdf/IF/IF10964/9.

[5] "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[6] Daniel R. Coats, "Worldwide Threats Assessment of the US Intelligence Community," Office of the Director of National Intelligence, Feb 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[7] United States Attorney's Office, District of Massachusetts, "Chinese National Arrested for Conspiring to Illegally Export U.S. Origin Goods Used in Anti-Submarine Warfare to China," Department of Justice, June 21, 2018, https://www.justice.gov/usao-ma/pr/chinese-national-arrested-conspiring-illegally-export-us-origin-goods-used-anti-submarine; United States Attorney's Office, Northern District of New York, "Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage," Department of Justice, January 3, 2023, https://www.justice.gov/usao-ndny/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage.

[8] Ellen Barry and Gina Kolata, "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?," The New York Times, February 6, 2020, https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html.

[9] Eamon Javers, "Chinese Company's Purchase of North Dakota Farmland Raises National Security Concerns in Washington," CNBC, July 1, 2022, https://www.cnbc.com/2022/07/01/chinese-purchase-of-north-dakota-farmland-raises-national-security-concerns-in-washington.html; Lars Erik Schönander and Geoffrey Cain, "China Is Buying the Farm," The Wall Street Journal, September 8, 2022, https://www.wsj.com/articles/the-chinese-are-buying-the-farm-north-dakota-hong-kong-land-food-shortage-supply-chain-usda-11662666515; Lillis, Katie Bo. "CNN Exclusive: FBI Investigation Determined Chinese-Made Huawei Equipment Could Disrupt US Nuclear Arsenal Communications." CNN, July 25, 2022. https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

This matters for our defense, as the PRC employs methods on American soil to funnel U.S. technology and know-how back to Beijing to advance its own military capabilities while also exploiting U.S. military vulnerabilities. The U.S. military's battlefield advantage has long rested on our superior technology. But that is at risk as Beijing seeks to close the gap in our technology advantage and become a world class military power, on par with the United States, by 2049.

This matters for American businesses. The Office of the Director of National Intelligence estimated in 2015 that the cost of economic espionage through hacking is $400 billion per year, largely attributable to the PRC. The Commission on the Theft of American Intellectual Property in 2017 estimated that the cost to the U.S. economy from stolen intellectual property (IP) could range from $225 to $600 billion annually.[10]

CCP law and policy further bolsters these methods. The CCP's military-civilian fusion (MCF) policy blurs the distinction between civil/commercial sectors and military/defense industrial sectors. It facilitates the transfer of technology and investments from the commercial sector to the military. Its national intelligence law, passed in 2017, requires that "all organizations and citizens shall support, cooperate with, and collaborate in national intelligence work… and shall protect national work secrets they are aware of."[11]

Finally, the PRC's advances in technology will undoubtedly also be fueled by its increase in research and development (R&D) expenditures and its science, technology, engineering, and math (STEM) workforce, both of which have trendlines that are increasing in China and decreasing in the United States. Data from the National Science Board shows that, over the 2000 to 2019 period, the U.S. share of global R&D declined from 37 to 27 percent while the share by China increased from 5 to 22 percent.[12] A recent study by Georgetown's Center for Security and Emerging Technology estimated that, by 2025, China's yearly STEM PhD graduates will nearly triple the number of U.S. graduates (in the same fields).[13]

The PRC challenge is one of both national and economic security. It is not only the pacing military threat for the United States, but also the top threat to U.S. technological competitiveness.

---

[10] Chris Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says," Bloomberg, November 18, 2015, https://www.bloomberg.com/news/articles/2015-11-18/no-sign-china-has-stopped-hacking-u-s-companies-official-says; "Update to the Report of the Commission on the Theft of American Intellectual Property," The National Bureau of Asian Research, February 2017, https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.

[11] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[12] Amy Burke et al., "The State of U.S. Science and Engineering 2022", National Science Board, January 18, 2022 https://ncses.nsf.gov/pubs/nsb20221/u-s-and-global-research-and-development.

[13] Remco Zwetsloot et al., "China is Fast Outpacing U.S. STEM PhD Growth," Center for Security and Emerging Technology, Georgetown University, August 2021, https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/.

Critical Infrastructure

The CCP is targeting critical infrastructure in the United States. I fully anticipate that – should a crisis or conflict unfold – Beijing would seek to disrupt the operations of critical infrastructure in the United States, especially early on. This could be motivated by a desire to deter U.S. action, affect U.S. decision-making, delay the mobilization of U.S. forces, or affect the will of the American people.

The DoD's annual military assessment of the PRC was stark in its assessment, "China seeks to create disruptive and destructive effects… to shape decision-making and disrupt military operations in the initial stages of a conflict by targeting and exploiting perceived weaknesses of militarily superior adversaries."[14] Both the DoD and Intelligence Community have further assessed that China could launch cyberattacks against critical infrastructure in the United States, such as oil and gas pipelines, and rail systems, that would disrupt service for days to weeks.[15]

The ransomware network hack of the Colonial Pipeline in May 2021, although not attributed to the PRC, provided a glimpse of what such disruptions could look like, with gas shortages, long lines at gas stations, and the panic buying that ensued. Similarly, the electrical grid failure in Texas in February 2021, also not the result of any PRC action, showcased the widespread impact of the loss of power for millions of Americans.[16]

The U.S. government has taken some steps to share intelligence information on PRC campaigns to target critical infrastructure. Notably, in July 2021, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released information on Chinese state-sponsored cyber intrusion campaigns, including tactics, techniques, and procedures (TTPs) that have been been employed with the aim of "holding U.S. pipeline infrastructure at risk" through physical damage to pipelines or disruption of pipeline operations.[17]

Influence Activities

The U.S. homeland is within reach of the PRC's influence activities. The PRC "conducts influence operations that target media organizations, business, academic, cultural institutions,

---

[14] "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," U.S. Department of Defense, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

[15] "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," U.S. Department of Defense, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF; "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 2022, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

[16] "The Timeline and Events of the February 2021 Texas Electric Grid Blackouts," The University of Texas at Austin's Energy Institute, July 2021, https://energy.utexas.edu/research/ercot-blackout-2021.

[17] "Cybersecurity Advisory: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, July 21, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a.

and policy communities of the United States."[18] As part of its "three warfares" concept, the PRC seeks to leverage psychological warfare, public opinion warfare, and legal warfare to influence decision-makers, shape public narratives, spread disinformation, and advance its interests.

Examples include TikTok, with over 100 million U.S. users that U.S. intelligence officials caution can be influenced by CCP-driven manipulation of its algorithms. They also include Operation Fox Hunt, where CCP-directed individuals spy on U.S.-based pro-democracy activists, intimidate Chinese and Chinese-American students at U.S. universities, and pressure individuals in the United States to return to China, including by threatening family members.[19] In contrast, Chinese state-run media characterize Fox Hunt as, "targeting suspected economic criminals, many of them corrupt officials."[20]

The PRC also exerts influence through its Belt and Road Initiative (BRI), including its Digital Silk Road (DSR) initiative, which involves a strategy of exporting terrestrial infrastructure, information and communications technology, and other high technology areas.[21] This global influence directly impacts U.S. businesses and U.S. security interests here at home.

One acute area of competition is in commercial satellite communications, which CSIS recently examined in a study on low Earth orbit (LEO) broadband networks.[22] These space-based constellations, such as SpaceX's Starlink and Amazon's Project Kuiper, offer a compelling solution for bridging the digital divide, specifically for rural and underserved communities, as nearly 40 percent of the world's population, and 28 percent of rural households in America remain unconnected. However, with its heavy economic presence in many BRI countries, China is positioned to negotiate concessions for its telecommunications and satellite broadband services, while discouraging the adoption of U.S. commercial services.

Further expansion of its telecommunications services could boost Beijing's presence in foreign terrestrial networks. This would provide the CCP with remote access to route data back to Beijing (as was reportedly done to the African Union Headquarters, whose network infrastructure was built and operated by Chinese entities), grant it extensive surveillance and

---

[18] "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," U.S. Department of Defense, September 4, 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.pdf.

[19] Office of Public Affairs, "Eight Individuals Charged With Conspiring to Act as Illegal Agents of the People's Republic of China," Department of Justice, October 28, 2020, https://www.justice.gov/opa/pr/eight-individuals-charged-conspiring-act-illegal-agents-people-s-republic-china.

[20] Cao Yin, "Success of Fox Hunt campaign continues," China Daily, November 5, 2015, http://www.chinadaily.com.cn/china/2015-11/05/content_22375920.htm

[21] Makena Young and Akhil Thadani, "Low Orbit, High Stakes: All in on the LEO Broadband Competition," Center for Strategic and International Studies, December 14, 2022, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221214_Young_LowOrbit_HighStakes.pdf?VersionId=vH1lp3dD7VcHGRcvuF9OdzV2WJc_KG42.

[22] Ibid.

coercive powers, enable it to block internet access or censor information, and exert greater control over international data flows.[23]

While the U.S. government has taken steps to ban Chinese telecommunications devices by Huawei, ZTE, and others, such high levels of dependence by other countries on Chinese-built and -operated digital infrastructure may lead to greater adoption of Chinese-crafted techno-authoritarian norms, standards, and data-governance practices.

Recommendations

Below are a few recommendations that I believe can help address these challenges.

- **Expand education and awareness.** This hearing is an important way to educate the American public that the threat posed by the CCP is not an abstract notion nor solely a distant military conflict that could take place across the Pacific. The American public and businesses need to understand the security and economic risks presented by the CCP and understand that they are a target of CCP influence and operations. Clearly, the U.S. homeland is not out of reach of Beijing's threats, with PRC malign activities and operations occurring here every day, below the level of armed conflict. The FBI now opens two new counterintelligence investigations nearly every day.[24] Should deterrence fail, the CCP is likely to ensure that the conflict is not contained in the Indo-Pacific but that it is felt in the United States, particularly through disruptions of critical infrastructure and influence campaigns.[25]

- **Deepen threat sharing with the private sector.** Building off CISA's work to-date, further expand threat intelligence sharing with the private sector. Encourage the downgrading of intelligence and provide security read-ons for business leaders across critical infrastructure sectors, e.g., energy, water, and financial services. Examples like the 2021 CISA advisory on oil and gas pipeline cyber threats, where specific TTPs attributable to Chinese state actors were shared, enable companies to better understand their vulnerabilities, the sophistication of adversary threats, and to make risk-informed decisions regarding protection and resiliency measures.

- **Transform counterintelligence (CI) and security missions.** CI and security missions have traditionally involved manual, labor-intensive processes, from espionage casework to background investigations for security clearances to defense industry site visits for inspections. The scale of the CCP threat, the various methods it uses for acquiring

[23] Abdi Latif Dahir, "China 'Gifted' the African Union a Headquarters Building and Then Allegedly Bugged It for State Secrets," Quartz, January 30, 2018, https://qz.com/africa/1192493/china-spied-on-african-unionheadquarters-for-five-years.
[24] Remarks by FBI Director Christopher Wray at the Ronald Reagan Presidential Library and Museum, January 31, 2022, Simi Valley, CA, https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122.
[25] "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," U.S. Department of Defense, September 4, 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.pdf.

technology, and the sheer volume of data that could be tapped into, necessitate adapting the tradecraft for these challenges. This includes incorporating new technologies, approaches to, and additional resources for the mission. For example, how can big data and artificial intelligence/machine learning (AI/ML) help identify supply chain vulnerabilities, monitor abnormal cyber activities, track foreign agents, and illuminate disinformation? How can CI analysts work with technology startups, on relevant business timelines, to prevent investment deals that involve adversarial capital?

- **Leverage technology innovation.** Maintaining U.S. technological leadership means not just preventing the transfer of technology to the PRC, but also setting the conditions for our innovation sector to prosper and to stay ahead of the competition. We are in a period of rapid technological change, with the commercial sector leading in many areas of technological innovation. The government should seek greater adoption and integration of commercial technologies to support mission needs, taking advantage of their speed, agility, and the private capital being invested in them.

- **Boost cooperation with allies and partners.** Our alliances and partnerships are a competitive advantage and source of strength that the CCP does not have. In order to lessen this advantage, China is actively trying to divide and weaken U.S. alliances and partnerships.[26] Our technology is soft power for the United States, and technology cooperation can be a strong feature of these relationships while also bolstering our private sector innovation base. But increasing cooperation will require revisiting U.S. technology control policies. We need to strike the right balance between protecting our sensitive technology, recognizing Beijing's extensive efforts to steal it, and enabling American companies to be the partner of choice for our allies and partners.

- **Continue investing in a strong defense.** Continued investment in a strong defense is required to deter PRC aggression, build resiliency to attack, and ensure we have the trained people, posture, intelligence, weapon systems, and munitions to defend the United States and the American people.[15]

Thank you again for your time today and I look forward to your questions.

# #

[26] Seth G. Jones, "Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense Industrial Base," Center for Strategic and International Studies, January 23, 2023, https://www.csis.org/analysis/empty-bins-wartime-environment-challenge-us-defense-industrial-base.