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.