COUNCIL on
FOREIGN
RELATIONS

March 17, 2026

SFS | GEORGETOWN UNIVERSITY
Walsh School of Foreign Service

Prepared Statement: For the Hearing "DeepSeek and Unitree Robotics: Examining the National Security Risks of PRC Artificial Intelligence, Robotics, and Autonomous Technologies and Building a Secure U.S. Technology Base."

Prepared statement by

Dr. Rush Doshi

Assistant Professor of Security Studies, Georgetown University Walsh School of Foreign Service
C.V. Starr Senior Fellow and Director of the China Strategy Initiative, Council on Foreign Relations

Before the

U.S. House Committee on Homeland Security, Cybersecurity and Critical Infrastructure Subcommittee
United States House of Representatives
2nd Session, 119th Congress
March 17, 2026

The following represents Dr. Doshi's prepared testimony:

Chairman Ogles, Ranking Member Swalwell, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today.

I am an assistant professor at Georgetown University's Walsh School of Foreign Service and C.V. Starr senior fellow at the Council on Foreign Relations, where I direct the China Strategy Initiative. I previously served on the National Security Council from 2021 to 2024, most recently as deputy senior director for China and Taiwan affairs. My academic work includes careful analysis of Chinese Communist Party texts and behavior, an approach I applied in *The Long Game: China's Grand Strategy to Displace American Order*, published by Oxford University Press.

My aim in this testimony is to explain the PRC's ambitions in robotics and artificial intelligence, the progress it has made relative to the United States, the risks of that progress, and what the United States might be able to do address it.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All statements of fact and expressions of opinion contained herein are the sole responsibility of the author.

I. PRC Aims and Advances in Robotics and Artificial Intelligence

Beijing has a grand strategy to displace U.S.-led international order. It seeks to "catch up and surpass" the United States technologically, to reduce its own dependence on others while increasing others' dependence on it economically through a policy of "dual circulation," and to acquire the military capability to defeat U.S. forces in a conflict.[1] Achieving these objectives requires winning what Beijing views as the fourth industrial revolution, and robotics and artificial intelligence are central to that objective.

A. Winning the Fourth Industrial Revolution

The Chinese Communist Party, drawing from Western literature on the subject, indicates in authoritative texts that there have been four industrial revolutions that determined the fate of nations. The first was steam power, and it led to British dominance. The second and third were electrification and mass manufacturing, which led to American dominance. And now we are in the fourth—AI, quantum, smart manufacturing, biotechnology—which China aims to win not simply for prosperity, but for relative power, too.[2]

That belief has fueled trillions of dollars in industrial policy, generational investments in scientific research and in education, and a comprehensive effort to dominate the technologies that will define the next century. As I've argued in prior testimony, Beijing employs a three-part playbook that combines its growing innovation capabilities and ample engineering talent with state support.[3] First, China acquires technology—purchasing foreign companies to access it, forcing technology transfer as a condition of market access, or stealing it through espionage. Second, it protects its home market through tariffs, non-tariff barriers, regulatory discrimination, and currency management, allowing domestic companies to build scale. Third, it wields industrial policy at a level that dwarfs anything elsewhere in the world—subsidies, tax breaks, directed research funding, cheap credit, and state investment—so that its companies can undercut rivals on price, capture market share (vice profit), and climb the value chain.

Driven by this strategy, China's share of global manufacturing has grown from 6 percent to 30 percent since the country joined the WTO, and its factories now produce nearly a third of all manufactured goods worldwide—more than the United States, Germany, Japan, South Korea, and the United Kingdom combined.[4] Robotic automation and artificial intelligence are deepening that advantage, not diminishing it. Similarly, China is the only other country in competition with the United States in AI, and many of its models are in the "top ten" for key benchmarks.

The scale of China's support for this effort is breathtaking. Beijing has likely stolen more than $1 trillion worth of U.S. intellectual property.[5] Its annual industrial support is conservatively estimated at approximately two percent of China's GDP—more than any other country and roughly twice the U.S. rate, or approximately $400 billion per year.[6] The U.S. Chips and Science Act, by comparison, provided approximately $50 billion across multiple years. Robotics and artificial intelligence are priorities within this agenda.

This strategy is reinforced by the China's Military-Civil Fusion (MCF) policy, which systematically integrates civilian and military technology development, applications, and production. Under MCF, products developed for commercial purposes might be simultaneously designed for potential military repurposing, for example, or nominally commercial acquisition of technology may quietly flow into military channels and capabilities. For these reasons, the line between a commercial robotics or AI company and a defense contractor is blurred.

B. Robotics Industrial Policy Efforts and Progress

Robotics is a top priority for China's leadership. In less than a decade, China has gone from a laggard in robotics to the global leader. This transition has been supported by dedicated industrial policy efforts.

In 2015, Beijing launched the "Made in China 2025" initiative, identifying robotics as one of ten strategic technology sectors and set domestic production and market share targets.[7] In 2021, it launched the 14th Five-Year Robotics Industry Plan, and established a goal of reaching an "international leading level," reducing reliance on foreign robots, and targeting revenue growth of 20 percent annually.[8] In 2023, it released a "Robotics Plus" action plan which included robot deployment mandates for manufacturing, healthcare, logistics, and education, among other sectors.[9] That same year, the Ministry of Industry and Information Technology issued detailed guidance on humanoid robotics, identifying specific technological bottlenecks and prioritizing breakthroughs in motion planning, cognitive AI, bionic sensing, and dexterous control systems.[10] Notably, this year, Beijing's most recent 15th Five-Year Plan draft outline elevates robotics and particularly "embodied intelligence" into one of the country's top ten "new industry tracks," treating it as an enabler across manufacturing, digital transformation, elderly care, and national security.[11]

In several categories of robotics, the progress is remarkable.

China is now the dominant force in industrial robotics by most measures. A decade ago, China relied on imported robots for nearly three-quarters of its domestic demand. Today, Chinese manufacturers produce nearly 60 percent of the country's industrial robots domestically.[12] In some industries, PRC industrial robots have a nearly 100 percent global market share. But not only is China producing these robots, it is also diffusing them through society at scale. In 2024, Chinese factories installed approximately 295,000 new industrial robots compared to 34,000 installations in the United States; China's installations were greater than the rest of the world combined.[13] There are now more than two million robots working in Chinese factories—five times more than in the United States. China has more than 30,000 smart factories, and its robotics market reached an estimated $47 billion in 2024 compared to a few billion dollars in the United States.[14] None of the world's top ten industrial robotics companies are headquartered in the United States.

In humanoid and other service robots, which are the frontier, Chinese firms now make up a vast majority of the estimated 16,000 humanoid robots sold globally in 2025.[15] Unitree's latest basic humanoid robot is priced at approximately $6,000, which is far below the cost of comparable American-made systems.[16] There are now dozens of Chinese companies making humanoid robotics compared to a handful of U.S. companies. And these cost advantages in humanoid robotics also extend to other "service" robots, including household variants.

China's advantages are not static. For example, China now accounts for approximately 60 percent of global AI-driven robotics patent filings, which will help it extend its lead. Between 2015 and 2022, China recorded a 545 percent increase in first-author robotics research publications, and it surpassed the United States in total robotics research publication volume in 2022[17] Beijing's National Development and Reform

Commission announced a $137 billion venture capital fund dedicated to robotics, AI, and advanced technologies over the next 20 years.[18] The central government launched an $8.2 billion National AI Industry Investment Fun.[19] PRC state banks also increased industrial lending by $1.9 trillion over the past four years, including for factory construction and, by extension, the installation of robots within them.[20] This created enduring demand-side support to purchase Chinese industrial robots, which in turn helped that industry achieve scale.

C. Artificial Intelligence Industrial Policy

China made AI leadership a stated national objective in its 2017 New Generation Artificial Intelligence Development Plan, which set out a roadmap to “achieve world-leading levels” and make China “the world’s primary AI innovation center” by 2030.[21] In the 14th Five-Year Plan, China shifted its focus to integrating AI into the economy via the "AI Plus" initiative.[22] The 2024–2027 “AI+ Manufacturing” effort mandates the deployment of 1,000 industrial intelligent agents and the creation of a national computing grid, emphasizing technological self-sufficiency and the replacement of traditional labor with embodied intelligence.[23] AI is a major focus of the new 15th Five-Year Plan, which includes the term more than fifty times, setting the target of integrating AI into 90 percent of the economy in this period.

China is increasingly competitive in AI. But unlike in robotics, where China’s manufacturing advantages pay rich dividends, China’s progress in AI is at least partially constrained by a lack of compute. Presently, China has commanding advantages in two of the three key inputs to AI development: energy and talent. China has more than two times the power generation of the United States. Last year, it added 500 gigawatts of power generation, or roughly eight times what the United States added in the same period.[24] On talent, China produces far more STEM graduates than the United States, and it has a domestic talent ecosystem that does not rely heavily on immigration.[25]

The one area where China lags, according to many analysts, is compute, particularly the stocks of advanced AI chips that allow for training and inference. This is by far the most important factor in artificial intelligence for training models and for running them, and the demand for compute is only increasing. According to research from Chris McGuire, among other analysts, the best U.S.-designed AI chips are currently around four to five times more capable than China’s best domestically produced chips, and they are made in much larger quantities than Chinese chips.[26] Moreover, China’s advanced chips, which come from its national champion Huawei, will not close the gap. Huawei’s own public roadmap suggests its next-generation chip will actually be less powerful than its current leading chip, which was the Huawei Ascend 910C. According to Nvidia and Huawei’s own public roadmaps, in two years the best Nvidia chip will be seventeen times more powerful than the best Huawei chip. Even with the most charitable assumptions in terms of Huawei’s production quantity, Huawei will probably be able to produce 1-4% as much compute as Nvidia will be able to produce in 2026, which suggests U.S. export controls on semiconductors and on the semiconductor manufacturing equipment that produce them are generally working to increase the U.S. share of global compute. The United States, in this way, maintains a critical chokepoint in AI over China; in contrast, China maintains many critical points over the United States in manufacturing.

PRC companies and leaders appear aware of this vulnerability. DeepSeek Founder Liang Wenfeng has indicated compute remains a significant bottleneck.[27] Leaders of several Chinese AI companies have warned that a lack of access to compute risked ceding the United States the advantage.[28] Chinese AI companies like Zhipu have seen shares fall more than 20 percent due to limited compute access.[29]

Chinese AI companies have tried to overcome this disadvantage in a number of ways. One is to smuggle chips from overseas, with Malaysia and Thailand and other countries now enormous consumers of U.S. AI chips.[30] Another is to access American leading edge chips remotely through the cloud, which remains legal. Still another method is what the industry calls model "distillation." Leading Chinese AI laboratories—including DeepSeek, according to Anthropic—have engaged in distillation attacks that use proxy networks and accounts to directly query American AI models and then replicate their capabilities at significantly reduced cost.[31]

The most significant moment in Chinese AI was the arrival of DeepSeek's models, which some called a "Sputnik" moment for the United States and its AI ecosystem. DeepSeek's algorithmic approach is truly impressive, and the lab has from its foundations as part of a private quantitative trading firm into a leading AI lab. Although a private company with an independent-minded founder, DeepSeek may ultimately have benefited from state support, and it has notable state connections that suggest it functions as a national champion. For example, despite reports that DeepSeek was able to train its model without U.S. chips, a Trump administration official indicated DeepSeek circumvented U.S. export controls by illegally training on smuggled Nvidia chips in Inner Mongolia, possibly with state support.[32] DeepSeek is integrated into China's National Supercomputing Network and its major telecom providers in ways that likely provide it still greater access to compute.[33] At a political level, the company's leadership has been included in top-level meetings with Premier Li Qiang and President Xi Jinping. Although DeepSeek is primarily funded by its founder and his successful hedge fund, it has been designated as a "National High-Tech Enterprise," granting it state subsidies. Congressional investigations have also revealed that DeepSeek's backend infrastructure is connected to China Mobile. Evaluations from the U.S. Department of Commerce, foreign governments, and independent researchers found that its model weights are structurally engineered to echo CCP narratives; per one report, this occurred four times more frequently than Western reference models.[34] In this sense, DeepSeek while still a private company is perhaps now better considered an AI "national champion" for China.

II. Risks to American Competitiveness and Security

Three distinct but related categories of risk demand this Committee's attention in robotics and artificial intelligence: risks of cyberespionage and cyber-attack; risks of manufacturing erosion and growing supply chain dependencies; and risks of dual-use spillovers for U.S. adversaries.

A. Cyberespionage and Cyberattack

I have previously testified at length before this Committee and the Senate Committee on Homeland Security on how the cybersecurity risks posed by PRC companies are not merely functions of individual corporate choices or specific software vulnerabilities but are instead structural, emanating from the legal architecture the PRC has constructed for private companies.[35] These challenges apply acutely in the robotics and AI sectors.

PRC Legislation

A complex web of PRC national security legislation makes it legally impossible for companies like Unitree and DeepSeek to operate as genuinely independent commercial actors. Four laws, among many others, are particularly significant. China's National Intelligence Law requires all citizens and organizations to "support, assist, and cooperate" with national intelligence work.[36] This is a legal obligation that can be invoked at any time, without judicial oversight, and without the company being permitted to disclose that it has been so compelled. The Data Security Law and the amended State Secrets Law require Beijing's approval for cross-border data flows and expand the definition of covered data to encompass virtually anything the state designates.[37]The Cybersecurity Law requires that data collected within China be stored on servers accessible to Chinese security services—which means operational data from U.S. facilities in China where Chinese robots are deployed could be made available to Chinese state authorities and could not necessarily be shared without permission with the U.S. parent company to improve American manufacturing.[38] The Encryption Law requires companies to hand over encryption keys to the State Cryptography Administration, removing any meaningful technical barrier between a company's data and the Chinese state, particularly in cloud computing.[39] Taken together, these laws mean that when a Chinese-manufactured robot is deployed in U.S. facilities, the company that built it is legally required to cooperate with Chinese intelligence services and legally prohibited from disclosing that it has done so.

Along with this legal framework, there is documented evidence of concerning activity. In particular, risks fall along two dimensions.

Cyberespionage Risks

The first is espionage. AI can strengthen cyber espionage efforts. Anthropic claims to have detected a PRC state-sponsored cyber actor executing an AI-orchestrated cyber espionage campaign. In this, case the PRC threat actor targeted approximately thirty global organizations including major technology companies, financial institutions, and government agencies using AI tools; the vast majority of operations were executed through agents independently at speeds beyond human capability.[40]

Add to this the outfitting of modern robotic platforms (from vehicles to humanoid robots to drones) with LiDAR sensors, microphones, and other sensing capabilities creates espionage risks. These sensors continuously generate precise, high-resolution three-dimensional maps of their operating environments and in many cases are accompanied by audio recording devices. Deployed in sensitive locations, and even American homes in the case of consumer robotics, that mapping capability could provide Chinese intelligence with a detailed picture of physical layouts, security postures, and patterns of activity, and so on. In the Philippines, Chinese intelligence operatives were caught using LiDAR sensors to map a U.S. military installation.[41] These risks have been identified in the robotics industry. Researchers have identified an undocumented access pathway in Unitree's Go1 quadruped robot allowing remote access to camera feeds and control functions without user authorization.[42] Separate research revealed that Unitree humanoid robots transmit data to servers in China at regular five-minute intervals.[43] In a notable recent case, a software engineer's effort to build his own remote-control app for a DJI robot vacuum revealed significant backend security vulnerabilities, allowing him to inadvertently access live camera feeds, microphone audio, maps, and status data from 7,000 other vacuums across 24 countries.[44] Backdoors have been found in a range of other connected devices. These include Yutong buses in Europe, which can be remotely deactivated, and Chinese-made medical devices sold in the United States that allow access to sensitive medical devices.[45]

Cyberattack Risks

The second risk is critical infrastructure attack and sabotage. The PRC has pre-positioned on the water, power, gas, telecom, and transportation networks upon which tens if not hundreds of millions American rely. In recent years, 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 compromised infrastructure providers in several sectors.[46] Previously, Deputy National Security Adviser Anne Neuberger explained, "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.[47] As Jen Easterly said to the Select Committee on the CCP, China 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."[48]

In this way, PRC-connected devices pose unusual risks in this respect. PRC industrial robots, electric vehicles, and drones could be sabotaged, causing catastrophic damage. As these machines become embedded in ports, energy plants, defense supply chains, hospitals, and government facilities, their compromise becomes a persistent and potent threat vector against critical infrastructure.

B. Industrial Competitiveness and Supply Chain Warfare

The second risk is related to U.S. competitiveness in manufacturing and emerging supply chain dependencies.

First, the United States could see catastrophic setback in manufacturing unless it is able to produce and adopt robots at scale. The robotics and AI booms of the coming decade could generate trillions of dollars in economic value, reshape global manufacturing, and determine which countries retain their industrial bases. If the United States and its allies and partners cede the robotics sector to China as they ceded solar panels, batteries, and electronics manufacturing, they may not recover. A country that cannot build robots will not be able to reap the physical-world benefits of the AI revolution, and may eventually be unable to build the things robots build. This creates the risk that U.S. manufacturing in other sectors will eventually wither away. The critical task is for the United States to produce and adopt this enabling technology at scale. Otherwise, it will miss the "fourth industrial revolution" and fall behind in industrial production.

Already, China's rapid dominance in industrial robotics is already accelerating the manufacturing advantage that allows it to manufacture at scale, even as labor costs rise and tariffs on Chinese goods increase.

Second, a related risk is growing dependence on China for robots and for the parts needed to build and maintain them. China has weaponized supply chain dependencies in rare earth minerals and magnets successfully against the United States. In the future, if the United States is unable to produce robots itself or the key parts they require, then dependence on China would be the logical outcome. For now, U.S. allies and partners, notably Japan, play a major role in the supply of parts for robots, but China is increasingly dominant and able to produce key inputs as actuators, reducers, and ball screws.

C. Dual-Use Applications

PRC leadership in various categories of robotics will have military applications. The availability of PRC robots in the United States allows these firms to achieve greater scale and greater profitability through high-margin sales, which in turn creates expertise and capacity for military purposes as well. Both the United States and China are considering military applications of various robots. For example, Chinese state media has broadcast footage of Unitree quadrupeds equipped with automatic rifles deployed in military training exercises.[49] At China's military parade in September 2025, armed "robot wolves" made a formal cameo appearance.[50] More broadly, the AI capabilities being refined for commercial applications—navigation, obstacle avoidance, terrain adaptation, target recognition—are directly applicable to autonomous weapons systems. Every Unitree robot deployed in an American warehouse is a revenue stream that funds military-adjacent R&D and a data source that accelerates the optimization of systems that may one day be turned against us. The United States should not provide the market revenue, deployment data, and iterative improvement opportunities that help Chinese companies optimize these capabilities for military use at the expense of its own industry and security. More broadly, an apart from robotics, AI models themselves have implications for warfighting. Already, militaries are attempting to incorporate models into decision support, logistics, and targeting. They also are used to help certain weapon systems operate more autonomously and intelligently in denied electromagnetic environments.

III. Policy Recommendations

Below follow recommendations for sustaining American leadership in robotics and artificial intelligence and reducing risks from China's advances in these areas. The recommendations are generally scoped to be within the jurisdiction of this Committee.

A. Extend and Strengthen Connected-Device Restrictions

Congress should codify and significantly extend the Information and Communications Technology and Services (ICTS) executive order framework to cover PRC-manufactured robotic systems.[51] Robotic platforms equipped with sensors, cameras, LiDAR arrays, and wireless connectivity present the same or greater risks as the connected vehicles that have already drawn regulatory attention. It is not advisable, for example, for Unitree robots to be employed in hospital settings or by U.S. government agencies. In addition to the ICTS authority at the Department of Commerce, the FCC also has authorities to take action in this space. Such an FCC approach might consider the "Trusted Partner" framework recently adopted by the FCC for uncrewed systems that involved broad prohibitions with a "blue" list for allied and partner suppliers. Regardless of what approach is ultimately taken, this Committee also should urge CISA to issue binding guidance prohibiting the deployment of PRC-manufactured robotic systems in critical infrastructure sectors—including ports, energy facilities, water treatment systems, and government buildings—and to conduct a comprehensive audit of where such systems are currently deployed.

B. Prohibit PRC Robotics and AI in Federal Procurement and Critical Infrastructure

Congress should enact legislation prohibiting federal agencies and federal contractors from procuring robotic systems or AI models developed by companies subject to PRC national security laws. Currently, the U.S. government actually treats some American companies, notably Anthropic, with greater scrutiny than PRC AI companies. And yet China's National Intelligence Law, Cybersecurity Law, Encryption Law, and Data Security Law together create legal obligations that no contractual arrangement or technical safeguard can reliably overcome, which is not true of U.S. AI companies. Procurement prohibitions in sensitive U.S. sectors, analogous to those enacted for Huawei telecommunications equipment, should be considered for robotic platforms and AI systems. Critically, such prohibitions should apply not only to direct federal procurement but also to subcontractors operating in sensitive supply chains and to operators of critical infrastructure who receive federal support or operate under federal license. Relatedly, Congress could consider creating a trusted AI and robotics certification framework—analogous to the first Trump Administration's Clean Network initiative in telecommunications.

C. Mandate Security Audits and Incident Reporting for Deployed PRC Systems

Congress should direct CISA to require operators of critical infrastructure to inventory and report all PRC-manufactured robotic systems and AI platforms currently deployed in their networks. Documented vulnerabilities demonstrate that security risks are real and present. Mandatory reporting requirements would give the federal government a clear picture of the exposure, and mandatory security audits would identify specific vulnerabilities. Operators who discover security issues through these audits should be required to report them to CISA and protected from liability for good-faith disclosures.

D. Limit PRC Access to American Compute

China has enormous advantages in the competition for the fourth industrial revolution: energy, talent, and especially the world's most advanced manufacturing system and the supply chain dependencies that this system allows it to exert over others. This was most powerfully demonstrated in PRC controls over rare earth minerals and magnets. In this environment, the main advantage that the United States retains is superior access to compute. This matters not only for AI training, but also for robotics: increasingly, the "brain" of the robot is "edge" computing that occurs on the device, which requires advanced chips; the "limbs" of the robot are manufactured in China, with key inputs from Japan. To maintain the U.S. advantage in compute, this Committee should signal support for the following. First, to close loopholes that allow China to access compute and frontier AI capabilities through cloud computing, API access, and third-country subsidiaries. Second, the United States should maintain and strengthen controls on access to semiconductor manufacturing equipment and advanced AI chips, and also consider expanding these controls to AI inference chips used in advanced robotics. This includes taking action against loopholes that facilitate smuggling and transshipment and bolstering allied and partner coordination on controls.

E. Build “Allied Scale” in Robotics

The United States cannot simply play defense. It also needs an affirmative strategy. In robotics, U.S. industrial policy is critical to ensure the capability to manufacture robots at scale. This means sustained support to the industry, including procurement programs that create demand; R&D funding to address technical challenges and breakthroughs; supporting technologies where “leapfrog” breakthroughs are possible over Chinese champions; and efforts to attract and retain the best talent in the industry. These are essential steps, but they are not sufficient without addressing PRC capacity. Presently, U.S. and allied and partner companies struggle to compete with PRC companies on price while continuing to depend on elements of China’s industrial ecosystem. The answer to this dilemma is to pursue domestic production alongside “allied scale” with partners to rival China’s enormous scale in this sector. The aim would be to create a common market for robotics among likeminded states that treats those within it better than the PRC. In particular, the United States should gradually incentivize companies to rely on U.S. and allied and partner supply chains, such as Japan’s, which will help them achieve scale relative to China and bring down costs. In parallel, the United States and its allies and partners should invest in indigenization. Recent successes in adjacent fields, including Ukrainian and Taiwanese efforts to build fully indigenous drones without Chinese parts, provide a potential model. And as the prior recommendations indicate, the United States should regulate, phase out, or consider banning PRC robots that might operate in sensitive U.S. sectors.

F. *CFIUS Reform*

Although CFIUS falls within the primary jurisdiction of other committees, there is an important homeland security nexus that warrants this Committee’s attention. To prepare CFIUS for the AI and robotics era, and the attendant risks to cybersecurity and critical infrastructure, Congress should shift from a reactive, transaction-based posture to a proactive technology protection strategy that secures the entire AI and robotics stack. This requires expanding the definition of critical technology to encompass the foundational layers of artificial intelligence—specifically sensitive training datasets, proprietary algorithms, and the specialized human capital targeted through "acquihiring" by foreign entities. Furthermore, current loopholes regarding non-controlling stakes and indirect transfers must be closed by mandating filings for any investment originating from countries of special concern, particularly China, regardless of the size of the equity share. By prioritizing the protection of dual-use innovations and tightening oversight on adversarial capital, we can ensure that the United States maintains its qualitative technological edge while remaining a global hub for trusted investment.

Thank you for your time. I look forward to your questions.

[1] Rush Doshi, The Long Game: China's Grand Strategy to Displace American Order (Oxford University Press, 2021). The formulation "catch up and surpass" (赶超) appears across a wide range of PRC party-state documents and leadership speeches.

[2] Doshi, The Long Game, Chapter 1; see also Doshi, testimony before the U.S. House Committee on Financial Services, February 25, 2025.

[3] See Doshi, testimony before the U.S. House Committee on Financial Services, February 25, 2025.

[4] Richard Baldwin, “China is the World’s Sole Manufacturing Superpower: A Line Sketch of the Rise,” VoxEU, Centre for Economic Policy Research, January 17, 2024; Doshi, testimony before the House Financial Services Committee, February 25, 2025.

[5] 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.

[6] Gerard DiPippo et al., “Red Ink: Estimating Chinese Industrial Policy Spending in Comparative Perspective,” Center for Strategic and International Studies, 2022; see also OECD industrial subsidy estimates.

[7] “Made in China 2025,” State Council of the People’s Republic of China, May 19, 2015, available at http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

[8] “14th Five-Year Plan for the Robotics Industry,” Ministry of Industry and Information Technology, December 28, 2021, available at https://www.gov.cn/zhengce/zhengceku/2021-12/28/5664988/files/7cee5d915efa463ab9e7be82228759fb.pdf .

[9] “Implementation Plan for the ‘Robotics Plus’ Application Special Operation,” PRC Central People’s Government, January 18, 2023, available at https://www.gov.cn/zhengce/zhengceku/2023-01/19/content_5738112.htm.

[10] “Guiding Opinions on the Innovative Development of Humanoid Robots,” Ministry of Industry and Information Technology, October 20, 2023, available at https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023.

[11] “China’s New Five-Year Plan Prioritizes Robotics. The World Should Pay Attention,” The Diplomat, March 14, 2026.

[12] “Is China Leading the Robotics Revolution?” ChinaPower Project, Center for Strategic and International Studies (CSIS), February 12, 2026, https://chinapower.csis.org/china-industrial-robots/; Jonas Nahm, “America Has an Edge Over China. Why Won’t We Use It?” New York Times, February 24, 2026.

[13] International Federation of Robotics, World Robotics 2025; Keith Bradsher and Meaghan Tobin, “There Are More Robots Working in China Than the Rest of the World Combined,” New York Times, September 25, 2025; Hugh Grant-Chapman et al., “Is China Leading the Robotics Revolution?” “Is China Leading the Robotics Revolution?” ChinaPower Project, Center for Strategic and International Studies (CSIS), February 12, 2026, https://chinapower.csis.org/china-industrial-robots/..

[14] “Is China Leading the Robotics Revolution?” ChinaPower Project, Center for Strategic and International Studies (CSIS), February 12, 2026, https://chinapower.csis.org/china-industrial-robots/.

[15] “Is China Leading the Robotics Revolution?” ChinaPower Project, Center for Strategic and International Studies (CSIS), February 12, 2026, https://chinapower.csis.org/china-industrial-robots/.

[16] Bradsher and Tobin.

[17] Sunny Cheung, “Embodied Intelligence: The PRC’s Whole-of-Nation Push into Robotics,” Jamestown Foundation, August 9, 2025.

[18] “Is China Leading the Robotics Revolution?” ChinaPower Project, Center for Strategic and International Studies (CSIS), February 12, 2026, https://chinapower.csis.org/china-industrial-robots/.

[19] Sunny Cheung, “China’s New Five-Year Plan Prioritizes Robotics; the World Should Pay Attention,” The Diplomat, March 12, 2026, https://thediplomat.com/2026/03/chinas-new-five-year-plan-prioritizes-robotics-the-world-should-pay-attention/.

[20] Keith Bradsher, “China Has an Army of Robots on Its Side in the Tariff War,” The New York Times, April 23, 2025,

https://www.nytimes.com/2025/04/23/business/china-tariffs-robots-automation.html

[21] “Full Translation: China’s ‘New Generation Artificial Intelligence Development Plan,’” New America Cybersecurity Initiative, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017. See also, Ministry of Industry and Information Technology (MIIT), "Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018–2020)," (December 2017), https://www.newamerica.org/insights/translation-chinese-government-outlines-ai-ambitions-through-2020/.

[22] This initiative was announced in the State Council of the PRC, “Government Work Report” (March 2024).

[23] MIIT et al., "Implementation Opinions on the 'AI + Manufacturing' Special Action (2024–2027)," (January 2026).

[24] Dan Murtaugh and David Stringer, "China’s Four-Year Energy Spree Has Eclipsed Entire US Power Grid," *Bloomberg*, January 28, 2026, https://www.bloomberg.com/news/articles/2026-01-28/china-s-four-year-energy-spree-has-eclipsed-entire-us-power-grid.

[25] Caroline Wang, “China Hit New Record of Solar and Wind Power Capacity Additions in 2024,” Climate Energy Finance, February 18, 2025; see generally Eva Roytburg, “AI Experts Return from China Stunned: The U.S. Grid Is So Weak, the Race May Already Be Over,” Fortune, August 14, 2025.

[26] Chris McGuire, "China's AI Chip Deficit: Why Huawei Can't Catch Nvidia and U.S. Export Controls Should Remain," Council on Foreign Relations, December 15, 2025, https://www.cfr.org/articles/chinas-ai-chip-deficit-why-huawei-cant-catch-nvidia-and-us-export-controls-should-remain.

[27] Jordan Schneider, "DeepSeek: The Quiet Giant Leading China's AI Race," *ChinaTalk*, November 27, 2024, https://www.chinatalk.media/p/deepseek-ceo-interview-with-chinas.

[28] Jane Zhang and Zheping Huang, "China AI Leaders Warn of Widening Gap With US After $1B IPO Week," *Bloomberg*, January 10, 2026, https://www.bloomberg.com/news/articles/2026-01-10/china-ai-leaders-warn-of-widening-gap-with-us-after-1b-ipo-week.

[29] "Zhipu AI Stock Slides as Compute Shortages Stall Global Expansion," *Tech in Asia*, February 23, 2026, https://www.techinasia.com/news/zhipu-ai-stock-slides-as-compute-shortages-stall-global-expansion.

[30] Mackenzie Hawkins, "U.S. Plans AI Chip Curbs on Malaysia, Thailand over China Concerns," *Los Angeles Times*, July 5, 2025, https://www.latimes.com/business/story/2025-07-05/u-s-plans-ai-chip-curbs-on-malaysia-thailand-over-china-concerns.

[31]Anthropic, "Detecting and Preventing Distillation Attacks," Anthropic News, February 23, 2026, https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.

[32] "China's DeepSeek Trained AI Model on Nvidia's Best Chip Despite US Ban, Official Says," Reuters, February 24, 2026, https://www.reuters.com/world/china/chinas-deepseek-trained-ai-model-nvidias-best-chip-despite-us-ban-official-says-2026-02-24/.

[33] "China's National Supercomputing Network Adopts DeepSeek's Model," *China Daily*, February 10, 2025, https://global.chinadaily.com.cn/a/202502/10/WS67a9ae74a310a2ab06eab396.html; Ben Jiang and Ann Cao, "China's Three Big Telecoms Operators Rush to Integrate DeepSeek Models into Cloud Services," *South China Morning Post*, February 10, 2025, https://www.scmp.com/tech/big-tech/article/3297961/chinas-three-big-telecoms-operators-rush-integrate-deepseek-models-cloud-services.

[34] Center for AI Standards and Innovation (CAISI), *Evaluation of DeepSeek AI Models Finds Shortcomings and Risks* (Washington, DC: National Institute of Standards and Technology, September 2025), https://www.nist.gov/system/files/documents/2025/09/30/CAISI_Evaluation_of_DeepSeek_AI_Models.pdf; Estonian Foreign Intelligence Service, *International Security and Estonia 2026* (Tallinn: Välisluureamet, February 2026), 72–75, https://www.valisluureamet.ee/doc/raport/2026-en.pdf; CrowdStrike Counter Adversary Operations, "Security Flaws in DeepSeek-Generated Code Linked to Political Triggers," *CrowdStrike Blog*, November 20, 2025, https://www.crowdstrike.com/en-us/blog/crowdstrike-researchers-identify-hidden-vulnerabilities-ai-coded-software/; Select Committee on the Chinese Communist Party, *DeepSeek Unmasked: Exposing the CCP's Latest Tool for Spying, Stealing, and Subverting U.S. Export Control Restrictions* (Washington, DC: U.S. House of Representatives, April 2025), https://chinaselectcommittee.house.gov/media/reports/deepseek-unmasked.

[35]Rush Doshi, testimony before the Senate Committee on Homeland Security and Governmental Affairs, September 24, 2024; Rush Doshi, testimony before the U.S. House Committee on Homeland Security, March 5, 2025.

[36]National Intelligence Law of the People's Republic of China, art. 7 (2017) ("All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with the law").

[37]Data Security Law of the People's Republic of China (2021); State Secrets Law of the People's Republic of China (amended 2024).

[38]Cybersecurity Law of the People's Republic of China (2017).

[39]Encryption Law of the People's Republic of China (2020)

[40]See Tarun Chhabra Testimony before the Senate Committee on Foreign Relations, https://www.foreign.senate.gov/imo/media/doc/5c78c941-bd21-2468-1d2c-957537481348/120225_Chhabra_Testimony.pdf

[41]Jack Burnham and Johanna Yang, "Philippines Busts Chinese Spy Ring Targeting U.S. and Allied Military Infrastructure," Foundation for Defense of Democracies, February 3, 2025.

[42]Sam Sabin, "Chinese Robotics Manufacturer Left Backdoor in Product," Axios, April 1, 2025; "Exploit Allows for Takeover of Fleets of Unitree Robots," IEEE Spectrum, September 25, 2025.

[43]"Unitree humanoid robots send data to China every 5 minutes, raising security fears," Interesting Engineering, October 1, 2025.

[44] Mack DeGeurin, "Man Accidentally Gains Control of 7,000 Robot Vacuums," *Popular Science*, February 21, 2026, https://www.popsci.com/technology/robot-vacuum-army/.

[45] Mark Lewis, "Norway's Capital Replaces Gas-Guzzling Buses with Electric Ones from China," *Associated Press*, January 12, 2024, https://apnews.com/article/ruter-yutong-china-norway-electric-buses-931f3dbdab3f82402da68cbcb31f856b; Cybersecurity and

Infrastructure Security Agency, *Contec CMS8000 Patient Monitor Contains a Backdoor*, CISA Fact Sheet (Washington, DC: Department of Homeland Security, January 30, 2025), https://www.cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf.

[46] 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*, Cybsersecurity & 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.

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

[48] 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.

[49]Jane Tang, "'The Robot Dog's Time to Kill': At China's Star Robotics Firm, the Military Ties Keep Mounting," The Brief (Kharon), July 16, 2025.

[50]"Weaponised 'robot wolves' make cameo at China military parade," The Guardian, September 5, 2025.

[51]See Rush Doshi, testimony before the Senate Committee on Homeland Security and Governmental Affairs, September 24, 2024.