STATEMENT BY
MAX FENKELL
GLOBAL HEAD OF POLICY AND GOVERNMENT RELATIONS
SCALE AI

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE CYBERSECURITY AND INFRASTRUCTURE PROTECTION

HEARING ENTITLED
“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"

MARCH 17, 2026

Chairman Ogles, Ranking Member Swalwell, and Members of the House Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, thank you for the opportunity to appear before you today. My name is Max Fenkell, and I serve as Scale AI's (Scale) Global Head of Policy and Government Relations. This hearing comes at a critical time for the future of United States leadership in artificial intelligence (AI), and I appreciate the chance to discuss the steps necessary to ensure the United States wins the global AI race.

INTRODUCTION

Over the past five years, no topic has captured global attention more than AI and since our founding in 2016, Scale has been at the forefront of AI innovation. Every day, our company works to build reliable AI systems for the world's most important decisions. We work across the entirety of the AI ecosystem, supporting customers from AI labs developing frontier models, to governments and enterprises looking to implement AI solutions. We do this in two main ways: first, by building high-quality, frontier data to develop, improve, and evaluate AI models; and second, by building applications to deliver solutions.

In the earliest days of our company, we started by building the Data Engine to power the autonomous vehicle industry. Later, that same Data Engine matured to serve as the foundational infrastructure to power the generative AI (GenAI) revolution; it now powers leading AI companies working to bring the technology into the physical world through robotics and autonomous systems. Our expertise in data has also enabled us to understand how to best implement our AI solutions across leading enterprises and governments, placing us at the forefront of AI deployment. Today, our Data Engine has powered the most ambitious Government AI programs, shaped the frontier of industry, and is actively working to power the next generation of agentic and physical AI platforms.

AI has always been powered by a data foundation, and winning on data will contribute to the US winning on AI. Scale directly enables this to occur.

WINNING STARTS WITH THE RIGHT STRATEGY

To start, it is useful to understand the AI tech stack. Across almost all use cases, AI fundamentally boils down to four parts: compute, model, data, and applications. Compute refers to the chips that power AI development and implementation; models are the engine that powers the AI to be useful; data is what makes the AI robust and intelligent; and applications leverage the rest of the tech stack to deliver high-quality AI solutions.

Understanding the state of the AI race requires examining leadership across each element of the tech stack. While the United States maintains an advantage on models and compute, China has established significant advantages in data and large-scale deployment. China continues to invest aggressively across the entire tech stack through an approach that fundamentally differs from the United States. The United States is chasing technological superiority, whereas China is looking to win on implementation[1] and diffusion of its technology across the world.[2]

As the AI industry continues to advance from a model-first approach to applications and embodied AI platforms, it is clear that the country that best implements AI solutions will reap the biggest benefit. Leadership in chips and models alone will not be sufficient. Without a stronger focus on implementation and deployment, the United States risks falling behind and never catching up.

ROBOTICS IS THE NEXT FRONTIER, BUT THE US IS NOT CURRENTLY IN THE RACE

Since the public release of generative AI systems in November 2022,[3] they have garnered much of the world’s attention. However, this represents only the beginning of the AI transformation. AI capabilities are already evolving beyond conversational systems towards agentic workflows, and the next wave of AI will see models shift from text-based to physical, powering real-world systems such as robotics. Winning on these systems requires a fundamentally different approach from the ground up, starting with how you train the models.

Training a Large Language Model (LLM) requires two foundational steps. The first is pre-training: training on publicly available data. The second is post-training: augmenting a pre-trained model with high-quality, human decisions to fine-tune and evaluate it. Once completed, that AI model is deployed through a user interface and constantly improved based on real-world feedback.

A physical AI system follows a different path. These systems require the collection of thousands of hours of real-world data prior to the labeling process. Once collected, that data is labeled, tagged, and annotated to build a high-quality Vision Language Action Model, and once deployed in a real-world environment, it is augmented by real world data to continuously improve.

This is why autonomous vehicles spend months driving city streets before launch – every mile is training data. For robotics, the equivalent is warehouse-scale facilities filled

[1] See, https://www.reuters.com/world/asia-pacific/china-vows-accelerate-technological-self-reliance-ai-push-2026-03-05/
[2] See, https://www.index.dev/blog/chinese-open-source-ai-models-statistics
[3] See, https://en.wikipedia.org/wiki/ChatGPT

with machines running around the clock, not to move goods, but to generate the data that trains the next generation of AI systems. China has industrialized this process in a way the United States has not. According to Scale's internal estimates, China owns roughly 90% of the commercially available robotics AI data industry today and produces it at 60% lower cost than U.S. companies can match. More investment alone will not close that gap. The advantage China has built is structural, state-directed, and years in the making.

The reason for this lies in China's approach. For many years, China has viewed data dominance as a key pillar of its AI Master Plan. While the U.S. Government directly invests roughly $100 million a year in AI data, China invests between 10x and 15x more, or roughly between $1 billion and $1.5 billion annually.[4] However, the difference extends beyond the investment levels.

China currently has seven data labeling hubs[5] across the country, provides government tax credits and subsidies for AI data,[6] and operates multiple of the world's largest warehouses with robots working up to 17 hours per day for the sole purpose of data collection.[7] This is not organic industrial development: it is a state-directed campaign to leverage the entirety of state capacity to control the foundational inputs of AI before the United States recognizes the threat.

The national security implications are clear. The same AI models being integrated into platforms and trained on Chinese data today are candidates for deployment in American homes, ports, hospitals, warehouses, and defense facilities tomorrow. The data that trains these systems shapes how they behave, what they optimize for, and where they are vulnerable. Ceding the robotics data layer to China is not an abstract technology policy concern, it is a critical infrastructure risk.

If the United States wants to win, we must recognize that the race is not just about platforms or technology superiority: we must also win on data. As with every form of AI, winning comes down to having a data advantage. Beyond global leadership, relying on Chinese data to train American companies' AI platforms carries significant security risks: supply chain issues, data poisoning[8], backdooring[9], and more. Unless we change our approach quickly, we will be almost entirely reliant on China to build America's robotics industry.

WINNING REQUIRES FOUR KEY ACTIONS

[4] These statistics are based on Scale's internal analysis of publicly available sources.

[5] See, https://www.globaltimes.cn/page/202404/1309974.shtml

[6] See, https://english.www.gov.cn/news/202501/14/content_WS67859ba1c6d0868f4e8eeca1.html

[7] See, https://robotsbeat.com/china-closes-robotics-gap-physical-ai/

[8] See, https://www.knostic.ai/blog/ai-data-poisoning?utm_source=chatgpt.com

[9] See, https://cybernews.com/security/dji-robot-vacuum-backdoor/

Given the state of the global AI race and China's clear strategic advantage, the United States must act with urgency. The United States is winning the AI race on the dimensions we can see — the models and the chips. We are losing it on the dimensions that will ultimately decide the outcome: data and implementation. Winning is not just about building the best technology; it is also about successfully deploying these systems across real-world applications. To achieve this, four actions are necessary:

First, investigate Chinese robotics data as a national security threat and treat U.S. data as a national asset. China's growing dominance in the robotics AI data raises significant national security concerns for U.S. industry, and an over-reliance on China to provide our leading companies with AI-ready data carries risks that should be carefully examined and mitigated. Further, we should explore how the U.S. Government's best-in-class data could be better leveraged as a strategic asset for AI leadership. Multiple National AI Strategies have called AI-ready data vital to advancing AI, and while progress has been made, more must be done to translate these commitments into action. China is taking a whole-of-government approach to winning on data. The United States must be prepared to match that intensity — and where possible, surpass it.

> Recommendation: Congress should immediately ask the National Security apparatus to study the risks associated with an over-reliance on Chinese robotics data. Additionally, Congress should require federal data assets be made AI-ready and put in place government-wide AI-ready data infrastructure to harness it.

Second, establish the right regulatory framework that maximizes innovation while putting in place guardrails where needed. The right framework will lay the groundwork for global leadership. Scale strongly believes that this system starts with a use-case-based approach that leverages the existing regulatory system, finding and filling gaps if they exist. The right model governs outputs, not inputs — just as the government does not regulate a laptop, it regulates the malicious use of a laptop. AI should be governed the same way. Where a regulation is sufficient, it requires clear implementation and compliance guidance, as well as third-party testing to verify compliance. Regulation that handicaps American AI companies is not sound policy; it is a strategic concession to Beijing.

> Recommendation: Congress should work to pass a legislative package that sets one national framework for AI governance and codifies the regulatory gap analysis approach.

Third, shift to an implementation-first mindset. As previously stated, the United States is pursuing technology superiority whereas China has an implementation-first mindset. This is most visible in government adoption for defense use cases. Since 2016, the Department of War has successfully transitioned only one AI program to a Program of Record. In contrast, China implemented 81 LLMs into People’s Liberation Army operations in the first half of 2024 alone.[10] This is true across the private sector as well. Recent studies show that only roughly 1 in 20 enterprise AI pilots reach production[11]. If we want to win, we must shift to an implementation-first approach.

> Recommendation: Congress should require federal departments and agencies to stand up at least five flagship agentic AI programs, or programs that leverage frontier AI capabilities to solve for individual use cases, no later than the end of 2028. The over 1,700 AI use cases already identified across the federal government make clear that agencies know where AI can be most effective — the barrier is not imagination, it is execution. Additionally, they should set up an interagency working group tasked and empowered to break down all barriers to government AI implementation and use every tool at their disposal to encourage private sector adoption of agentic AI solutions.

Fourth, export the AI tech stack to our allies and partners. For too long, the United States has allowed China to dominate global tech exports through initiatives like the Belt and Road Initiative and Digital Silk Road,[12] which saw China win on 5G. This has led to China's technology becoming the global standard around the world and this cannot happen on AI. Countries around the world, or AI geopolitical swing states, will soon be forced to choose between deploying Western or Chinese technology. The Trump Administration has taken critical steps to counter China's exports around the world through the "Promoting the Export of the AI Technology Stack"[13] Executive Order, but this must only be a starting point. It is critical that Congress codifies key provisions from this Executive Order and ensures that the Departments of State and Commerce are resourced to effectively carry out their mandates. Global leadership on AI starts with becoming the global standard.

> Recommendation: Congress should immediately work to codify this Executive Order and ensure adequate funding for the Agencies tasked with implementing it.

CONCLUSION

The AI race will not be won in a laboratory or manufacturing plant alone. It will be won through the strategic decisions we make today. This is not the first time America has faced a defining technological competition, and we have every asset required to win: the talent, the capital, and the allies. The variable is urgency.

[10] See, https://www.scmp.com/tech/tech-trends/article/3267866/chinas-public-sector-accelerates-ai-adoption-2024-zhipu-and-iflytek-emerge-winners

[11] See, https://fortune.com/2025/08/18/mit-report-95-percent-generative-ai-pilots-at-companies-failing-cfo/

[12] See, https://www.cfr.org/china-digital-silk-road/

[13] See, https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/

Despite years of strong rhetoric, a clear-eyed understanding of where this race is actually being run has been missing. It is being run on data and implementation, and without direct action, we will lose.

The window to act is open, but it will not remain open indefinitely.

Scale is fully committed to supporting the United States in the global AI race. We look forward to working with this Committee to find ways to do just that.

Thank you again for the opportunity to be here and I look forward to your questions.

Testimony of Matthew Malchano,
Vice President of Software

Before the
United States House of Representatives
Homeland Security Committee
Cybersecurity & Infrastructure Protection Subcommittee

Hearing on the topic of
"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"

March 17, 2026

Chairman Ogles, Ranking Member Swalwell, and distinguished members of the subcommittee. Thank you for the opportunity to testify on this very important and timely topic. I am Vice President of Software at Boston Dynamics, the world's leading developer of advanced mobile robots. I also serve as the company's Security Officer, responsible for overseeing our cybersecurity and data sovereignty protocols. Having worked for the company for 22 years in leadership and technical roles, on both commercial products and government projects, I have witnessed our industry's transition from its initial era of academic experimentation, to government-funded research projects, to early commercial deployment and, now, to a company that is engaged in one of the most consequential global competitions in advanced technology.

Our company, founded over 30 years ago by a Massachusetts Institute of Technology professor and his students, is at the forefront of an industry which will result in advanced mobile robots becoming common in industrial, public safety, entertainment, defense and security applications. Advanced mobile robots are still a new technology, but our robots are already in use in manufacturing facilities, semiconductor fabrication plants,[1] energy plants,[2] as well as in police departments. One of our robots has even taken bullets in the line of duty.[3] Our robots are

[1] See Global Foundries Case Study, available at https://bostondynamics.com/case-studies/globalfoundries/.

[2] See Meet Chevron's New Energy Watchdog, available at https://bostondynamics.com/case-studies/meet-chevrons-new-energy-watchdog/.

[3] See "Robotic police dog shot multiple times, credited with avoiding potential bloodshed," Associated Press, March 27, 2024, available at https://apnews.com/article/massachusetts-cape-cod-robot-dog-police-f63586d5286750702f396109c9a81836.

used by the United States Secret Service to protect the President,[4] and by military agencies to investigate and neutralize the threat of improvised explosive devices.[5] We are headquartered in Massachusetts, with a growing workforce of over 1,000 employees, and we proudly design and manufacture our robots in the United States.

Exciting recent advances in AI are already accelerating the development of a new generation of mobile robots. Computer vision enables robots to perceive their environment, recognize objects, and offer contextually relevant services. Vision and natural language processing will enable us to more easily communicate with robots using language and gestures. Motion control software, created by machine learning and reinforcement learning, increasingly drives the robots, accelerating their development. Robots now learn tasks using AI technologies to observe and analyze the movements of people or other robots doing that task.[6] But these advances in AI also enable competitors, including those headquartered in foreign adversarial nations, to quickly close the gap in capabilities. Their robots and ours can now be built and programmed in 30 months to do what our company once took 30 years to develop.

The New Generation of Robotics Raises Economic Security and National Security Risks

The types of products or machines that could be described as a "robot" are very broad. I focus my testimony on what I call *advanced robotic technologies*. *Advanced robotic technologies* consist of highly agile mobile robots designed to be put to work in a variety of environments and applications, and whose functionality is trained by, or enhanced by, artificial intelligence methodologies. These types of robots raise heightened economic security interests and national security risks, and therefore should most squarely be the focus of federal policy, for the following reasons:

1. **Advanced robotic technologies are dual-use.** A robot developed to navigate complex environments, using legs or other methods providing enhanced agility and dexterity, will eventually be useful in the battlefield. Just in the past few months, we have seen Chinese-made quadrupeds exhibited during China's military parade,[7] and videos of Chinese humanoids training to fight in hand-to-hand combat.[8] There have also been reports of quadrupeds, developed by Chinese robotics companies including the company identified in the title of this hearing, armed with machine guns and used

[4] See "Robotic dogs are patrolling Mar-a-Lago to help protect Trump, Secret Service confirms," FOX 59, November 8, 2024, available at https://fox59.com/news/national-world/robotic-dogs-are-patrolling-mar-a-lago-to-help-protect-trump-secret-service-confirms/.

[5] See "Boston Dynamics Awarded Contract to Supply Spot to the Dutch Ministry of Defence,"available at https://bostondynamics.com/blog/boston-dynamics-awarded-contract-to-supply-spot-to-the-dutch-ministry-of-defence/.

[6] For a recent explanation from our robotics AI team of how we are using AI to make robots more capable than ever before, with accompanying illustrative videos, please see "Large Behavior Models and Atlas Find New Footing," Boston Dynamics, available at https://bostondynamics.com/blog/large-behavior-models-atlas-find-new-footing/ .

[7] See "Weaponised 'robot wolves' make cameo at China military parade," The Guardian, September 5, 2025, available at https://www.theguardian.com/world/video/2025/sep/04/weaponised-robot-wolves-make-cameo-at-big-china-military-parade-video.

[8] See "China Just Held the First-Ever Humanoid Robot Fight Night," Vice.com, May 27, 2025, available at https://www.vice.com/en/article/china-just-held-the-first-ever-humanoid-robot-fight-night/.

in joint military training exercises in Cambodia.[9] And of course, U.S. forces have been using mobile robots for years to investigate and mitigate IEDs. Robots with enhanced mobility and AI-powered capabilities will be even more important in military applications, and we have seen in recent years how *aerial* robotics (drones), including those designed and intended for commercial or consumer use, can become consequential, or even outcome-determinant, in warfare.[10] Therefore, ensuring the success and growth of the domestic advanced robotics industry, including ground robotics systems designed and developed for commercial and industrial applications, is of national security importance.

2. **Advanced robotic technologies are increasingly crucial in the manufacture, production, and supply chain of other goods.** These technologies will help address workforce shortages of the future due to demographic inevitabilities arising from diminishing birth rates in the United States and elsewhere. Humanoids and similar form factors allow for automated physical operations in workspaces designed and built for humans, allowing existing infrastructure and factories to remain in operation even during labor shortages. The countries that build and deploy these advanced robots will be the ones that are best poised to manufacture on their own shores efficiently, and to protect their supply chains in other industries including automobiles, ships, defense materiel, and rail cars. Manufacturing in these other sectors has already been recognized by the federal government as being of national security importance to the United States. The robots that *enable and sustain* such manufacturing are a matter of economic security as well. Fast, agile manufacturing is, in turn, a key flywheel for advanced research and development. It is likely that robot acceleration may create a run-away amplification effect for technology development and industrial dominance.

3. **Advanced robotic technologies are the physical embodiment of artificial intelligence.** Various officials in the United States government have rightfully emphasized the need for the United States to win the AI race. Advanced robots are the physical manifestation of AI, leveraging everything from computer vision and reinforcement learning to visual language action and large behavior models -- to learn how to interface with the real world and perform a wide range of useful tasks. Some of these tasks will have national security importance. Even if the United States leads on software AI, the potential for dominance of robotic hardware by foreign adversaries will create national security vulnerabilities. If U.S.-sourced software can

[9] See "Meet the Chinese army's latest weapon: the gun-toting dog," The Guardian, May 30, 2024, available at https://www.theguardian.com/science/article/2024/may/30/chinese-armys-latest-weapon-gun-toting-dog.

[10] "Ukraine Says More Than 80% of Enemy Targets Now Destroyed by Drones," Defense News, January 28, 2026, available at https://www.defensenews.com/global/europe/2026/01/28/ukraine-says-more-than-80-of-enemy-targets-now-destroyed-by-drones/ .

only be deployed in machines that have been produced elsewhere because of the erosion of the domestic robotics industry, AI-only security will be insufficient. To win the AI race, the United States must win the robotics race.

4. **Using foreign advanced robotics technology in critical roles creates a risk of interference, access, and denial of service.** The unique combination of hardware, software, sensors, mobility, and communication mechanisms makes advanced mobile robots higher risk than other internet-of-things technologies, and it can be practically impossible to rule out tampering by adverse interests if done by the manufacturer. As robots become a critical part of key infrastructure, they become a potential and potent threat vector to that infrastructure.

Other Nations, Including U.S. Adversaries, Are Prioritizing Robotics

The economic, strategic and national security importance of robotics is evident from efforts made by other nations to support and promote their domestic robot industries. Nations that have implemented some form of national strategy initiative for robotics include Japan, South Korea, Singapore, Germany, France, the Netherlands, India and China. *See* "A Time to Act: Policies to Strengthen the US Robotics Industry," Information Technology & Innovation Foundation, July 18, 2025, available at https://itif.org/publications/2025/07/18/time-to-act-policies-to-strengthen-us-robotics-industry/.

Recent events demonstrate that China, especially, has recognized the national security implications of its advanced robotic technologies sector. In February 2025, the CEO of prominent Chinese robotics company Unitree, which develops and manufactures quadrupeds and humanoids, was seated prominently across from Chinese President Xi at a summit of tech executives. *See* "What did China's tech entrepreneurs tell Xi Jinping at the symposium?" *South China Morning Post*, February 21, 2025, available at https://www.scmp.com/tech/big-tech/article/3299599/what-did-chinas-tech-entrepreneurs-tell-xi-jinping-symposium. China also recently hosted a humanoid half-marathon and humanoid "Olympics." *See* "China's robots race against humans – and their U.S. counterparts," *NBC News*, April 23, 2025, available at https://www.nbcnews.com/news/world/china-robots-race-humans-half-marathon-rcna195586; "Tesla Optimus rival Unitree shines at the 'World Humanoid Robot Games' in China," *CNBC*, August 18, 2025, available at https://www.cnbc.com/2025/08/18/world-humanoid-robot-games-china-tesla-unitree.html.

The elevation of China's robotics community onto its national stage is not accidental. Instead, it is a direct consequence of comprehensive government support of China's robotics industry and AI-driven innovations. For example, we note the PRC's "Fourteenth Five-Year Plan for the Robotics Industry" (2021-2025), Central People's Government, December 21, 2021, available at https://www.gov.cn/zhengce/zhengceku/2021-12/28/content_5664988.htm as well as its "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. These documents outline the many mechanisms and policies that have supported the Chinese robotics industry, ranging from government funded R&D, to tax deductions, to government acting as first adopters to SOE robot procurement prioritization. *See also* China M.I.I.T. "Guiding Opinions on the Innovative Development of Humanoid Robots," Center for Science and Technology Innovation (Beijing), November 3, 2023, available at https://www.ncsti.gov.cn/zcfg/zcwj/202311/t20231103_140346.html.

Commentators and experts have evaluated the impact of these policies on the industry. *See, e.g.*, "America Is Missing The New Labor Economy – Robotics," *SemiAnalysis*, March 11, 2025, available at https://semianalysis.com/2025/03/11/america-is-missing-the-new-labor-economy-robotics-part-1/ (indicating that there is "an existential threat to the US as it is outcompeted in all capacities"); "The Humanoid 100: Mapping the Humanoid Robot Value Chain," Morgan Stanley, available at https://advisor.morganstanley.com/john.howard/documents/field/j/jo/john-howard/The_Humanoid_100_-_Mapping_the_Humanoid_Robot_Value_Chain.pdf ("Our research suggests China continues to show the most impressive progress in humanoid robotics where startups are benefitting from established supply chains, local adoption opportunities, and strong degrees of national government support."); "How Innovative Is China in the Robotics Industry?," Information Technology & Innovation Foundation, available at https://itif.org/publications/2024/03/11/how-innovative-is-china-in-the-robotics-industry/ ("China had 12 times the rate of robot use in manufacturing than did the United States."); Testimony of Sunny Cheung, Jamestown Foundation, before the U.S.-China Economic and Security Review Commission, February 6, 2025, available at https://www.uscc.gov/sites/default/files/2025-02/Sunny_Cheung_Testimony.pdf ("The results of these sustained efforts are evident in the rapid rise of leading Chinese robotics companies such as UBTech, Fourier Intelligence, Unitree Robotics, and major tech giants like Xiaomi and XPeng, which have expanded into humanoid robotics development. These companies are increasingly competitive in global markets, not just as adopters of automation but as innovators producing cutting-edge robotic systems with intelligent AI integration."); *Embodied Intelligence: The PRC's Whole-of-Nation Push into Robotics*, Sunny Cheung, Jamestown Foundation, August 9, 2025, available at https://jamestown.org/program/embodied-intelligence-the-prcs-whole-of-nation-push-into-robotics/ ("The rise of the PRC's robotics industry represents a tightly coordinated, whole-of-nation campaign driven by national strategy, regional policy alignment, and deep industrial integration.").

National strategies in Chinese industry policy are often executed via government subsidies at the local or provincial level. *See Far From Normal: An Augmented Assessment of China's State Support,* Rhodium Group, March 17, 2025, *available at* https://rhg.com/research/far-from-normal-an-augmented-assessment-of-chinas-state-support/ ("China spends more through direct grants and tax benefits than any other major economy, both in absolute amounts and as a share of GDP"). "China's industrial policy spending is enormous, totaling at least 1.73 percent of GDP in 2019. This is equivalent to more than $248 billion at nominal exchange rates and $407 billion at purchasing power parity exchange rates." See "Red Ink: Estimating Chinese Industrial Policy Spending in Comparative Perspective," Center for Strategic & International studies, available at https://www.csis.org/analysis/red-ink-estimating-chinese-industrial-policy-spending-comparative-perspective According to Jamestown Foundation's research, State-sponsored overproduction is another policy-driven approach that will have an impact on the robotics sector. *See, e.g., Beyond overcapacity: Chinese-style modernization and the clash of economic models,* Mercator Institute for China Studies, April 1, 2025, available at https://merics.org/en/report/beyond-overcapacity-chinese-style-modernization-and-clash-economic-models (indicating that "advanced industrial machinery and components" is one of the sectors most likely to see overcapacities emerge due to Chinese government policy). China has used state-backed financing to boost its intelligent robotics industry, offering tens of millions of dollars in subsidies, loans and other financial support. "[P]rovinces and cities [in China] are engaged in a de facto 'subsidy race,' each vying to foster the next national robotics champion within their jurisdiction." *Id*.

One example of Chinese government support that we have been able to trace is the "little giant" designation. Enterprises that secure a national designation from China's Ministry of Industry and Information Technology (MIIT) as specialized, refined, distinctive, and innovative "little giant" firms are eligible for provincial funding, reduced corporate income tax rates, accelerated depreciation of R&D equipment, and matching grants for innovation projects. Our research of sources in China indicates that various leading Chinese robotics companies have received the so-called "little giant" designation, including Unitree but also DEEP, Fourier, Leju, Qiteng, and Tianlian. This designation signals their ability to access a wide range of government funding and support. Indeed, a recent Guangdong province policy document, "Notice on Organizing the Project Entry of Specialized, Refined, Distinctive, and Innovative 'Little Giant' Enterprises in the Field of Artificial Intelligence and Robotics" (September 2, 2025), outlines subsidies for designated "little giant" enterprises specifically in the field of AI and robotics. It is evident that China's robotics producers have been the beneficiaries of state subsidies and support.

China is proceeding expeditiously with its government-sponsored industrial strategy. As just one example, in November 2025, the Chinese government formed an advisory committee on humanoid robotics, overseen by the Ministry of Industry and Information Technology, and appointed the CEOs of Unitree and AgiBot as co-chairs.[11] By March 2026, barely three months later, working together with 120 research institutions, the committee had already developed and released a six-pillar national standard for humanoid robotics, described as the "first

[11] "Unitree, AgiBot founders, China's robotics stars, join panel to shape industry standards," South China Morning Post, November 25, 2025, available at https://www.scmp.com/tech/policy/article/3333964/unitree-agibot-founders-chinas-robotics-stars-join-panel-shape-industry-standards .

comprehensive, top-level design covering the entire industrial chain and full lifecycle of humanoid robotics and embodied intelligence."[12]

China's strategy for advanced robotic technologies mimics the same approaches that it has used in other technology sectors: marketing products at prices which can only be possible by government support, intentionally over-produced and/or sold below cost. If left unchecked, over time, the impact of China's state support will echo in robotics the results seen in unmanned aircraft systems (drones): producers in the United States will struggle to compete, lose sales due to price differentials, and eventually many of them may be forced to drop out of the market.

Due to the nascent nature of the advanced robotic technologies industry, these impacts have yet to be felt in the U.S. industrial sector, but they have become evident in research universities and academic institutions, who are typically the early adopters of such technologies. Boston Dynamics' Spot robot dominated this research market from 2020-2022. However, in only the past 12-18 months, advanced robotic technology uses in that market have become dominated by the less-expensive and less-featured Chinese brands, particularly Unitree. This rapid shift in the academic/research market foreshadows the potential future dominance of foreign producers of advanced robotic technologies across other sectors worldwide, such as manufacturing, energy, logistics, security patrol, law enforcement, and even defense. Indeed, we are already seeing a notable increase in adoption of Chinese quadruped robot "dogs" by domestic law enforcement agencies, similar to the early years of Chinese drone adoption by law enforcement agencies.[13] Additionally, network effects here mean that as a platform becomes dominant in the new market, new capabilities and applications will favor that platform, leading to a substantial first mover advantage.

The role of robotics across key industrial sectors, and the extent of the Chinese government's support for robotics, are starkly revealed by the Chinese government's new five-year plan, released earlier this month in Beijing. Robotics "now commands its own dedicated inset box among the plan's top ten 'new industry tracks.'" *China's New Five-Year Plan Prioritizes Robotics. The World Should Pay Attention*, The Diplomat, March 14, 2026.

> [R]obotics is not treated as a standalone sector but as an enabler woven across chapters on manufacturing, digital transformation, elderly care, national security, and even cultural development. This is less an industrial policy *for* robots than an industrial policy *through* robots.
>
> *Id*. (emphasis in original).

[12] "China's first national standard system for humanoid robotics poised to spur industry development," Xinhua, March 3, 2026, available at https://english.news.cn/20260303/0e51ac8f66c542c5bacf2af3f80b3a40/c.html .

[13] US police departments and public safety agencies that have recently adopted Chinese "robot dog" models include Brawley Police Department (California), Charles County DES (Maryland), Topeka Police Department (Kansas), Pullman Police Department (Washington), and Port St. Lucie Police Department (Florida).

This new plan makes clear that the full support of the Chinese government now stands behind its robotics sector, including "access to the 60 billion RMB ($8.2 billion) National AI Industry Investment Fund, provincial matching funds, and the full apparatus of state-backed venture capital." *Id*. These efforts are currently unmatched by any policy efforts in the United States to support its domestic robotics industry.

The Nature of the Cybersecurity Threat

Robots that are not secure and that contain cyber vulnerabilities, especially those produced by adversarial actors, pose a variety of serious risks to the facilities and/or agencies that deploy them.

Advanced mobile robots present new and unique classes of cybersecurity risk beyond AI and computer systems. These robots are complex systems made of software and hardware. When produced by adversarial nations they carry larger probabilities of being compromised with backdoors and remote access allowing nation-state attackers (intelligence or military) to take control. If compromised robots become critical components of in turn security critical systems, attackers can sabotage those systems, interfere with a manufacturing line or halt a security patrol. As robot capabilities approach those of humans in terms of seeing, moving, and manipulation, a compromised robot gives attackers eyes and hands throughout sensitive facilities. Growing autonomy lets these robots take actions on their own.

Public security researchers have additionally demonstrated clear gaps in Chinese manufactured robot security. Even in the absence of specific attack intent, these vulnerabilities open users of these systems to potential third party attacks.

Securing systems that are used in high-value or sensitive operations should be a priority for both engineers and nations. Boston Dynamics has set out our approach to securing robots in a whitepaper describing how we maximize the security of our products, including the features and design considerations which enable these platforms to be trusted parts of customer IT integrations. See https://bostondynamics.com/wp-content/uploads/2024/03/spot-and-site-hub-security-white-paper.pdf

Unitree: One of Many Companies Raising Concerns

This hearing's title calls out Chinese robotics company Unitree specifically. To be sure, Unitree has been the most visible company marketing and selling its legged robots in the United States, and also appears to have been chosen by the government of China as a national champion. News media have reported cybersecurity vulnerabilities in the company's products, including data exfiltration exploits and remote-control backdoor access.[14] Additional security research

[14] See "Exploit Allows for Takeover of Fleets of Unitree Robots," IEEE Spectrum, Sept 25, 2025, available at https://spectrum.ieee.org/unitree-robot-exploit and "Unitree humanoid robots send data to China every 5 minutes,

relating to Unitree robots that did not receive wide press coverage include a reported exploit that enables a network-based takeover of the robot and the discovery of a reported Unitree AI/LLM cloud service that could cause arbitrary commands to be executed on the robot.[15] The company also seems to be widely engaged in white labeling products that appear in the United States under different brand names.[16] A few weeks ago, following earlier reports of connections between Unitree and the PLA,[17] Unitree was placed on the Department of War's Section 1260H list of Chinese Military Companies, before that list was withdrawn (apparently, temporarily and not for reasons related to Unitree).[18] Most recently, forty-nine Unitree humanoids performed at a high profile Spring Festival spectacular, dancing rhythmically, vaulting, breakdancing, and mock sword fighting, showing a high degree of confidence in placing fast-moving robots next to child performers before a live audience. Unitree is also moving forward with an initial public offering this year. Given its market penetration, reported security vulnerabilities, and apparent ties to the Chinese government and military, it is not surprising that Unitree has earned the focus and attention of the US government, security analysts and policymakers. Scrutiny by this subcommittee is certainly warranted.

However, there are literally dozens of other Chinese companies making rapid progress with government support, particularly in the humanoid space. At the 2026 Consumer Electronics Show in Las Vegas, where we debuted the new version of our Atlas humanoid robot, Chinese companies displaying humanoid robots appeared to outnumber US companies by a factor of five to one. On social media, industry observers are tracking dozens of Chinese humanoid companies, compared to just a handful in the United States:

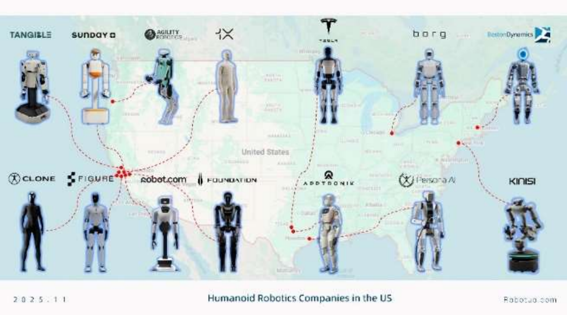
raising security fears," Interesting Engineering, October 1, 2025, available at https://interestingengineering.com/innovation/security-flaw-unitree-humanoids-china .

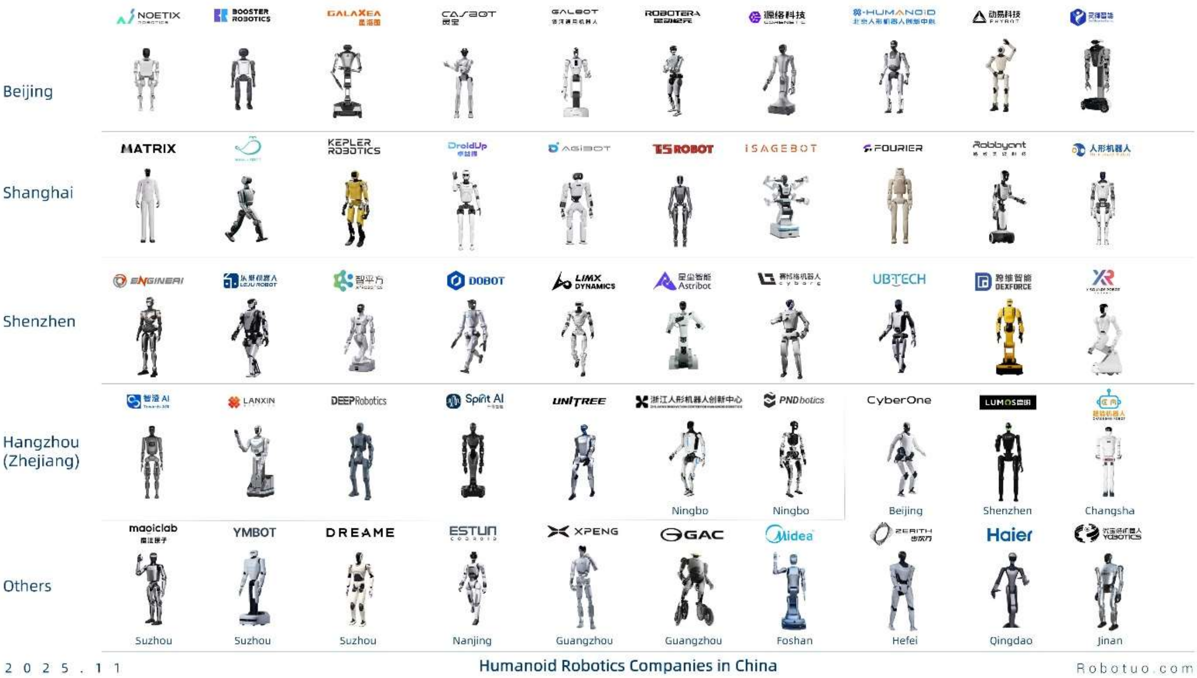
[15] For the original research reporting these issues, see: "The Jailbroken Unitree Robot Dog ," available at https://www.darknavy.org/darknavy_insight/the_jailbroken_unitree_robot_dog/; "39C3 - Skynet Starter Kit: From Embodied AI Jailbreak to Remote Takeover of Humanoid Robots," available at https://www.youtube.com/watch?v=qjA__5-Bybs ; "Skynet Starter Kit – Researchers control humanoid robots via radio & AI," available at https://www.heise.de/en/background/39C3-Skynet-Starter-Kit-Researchers-control-humanoid-robots-via-radio-AI-11125615.html .

[16] One example is a flamethrower-equipped quadruped robot sold by a company called Throwflame, which is obviously a white-labelled Unitree robot. https://throwflame.com/products/thermonator-robodog/ . Another company, Robot.com, is using rebranded Unitree robots for urban delivery. https://www.robot.com/ .

[17] "'The Robot Dog's Time to Kill': At China's Star Robotics Firm, the Military Ties Keep Mounting," Kharon The Brief, July 17, 2025, available at https://www.kharon.com/brief/unitree-robotics-china-pla .

[18] "U.S. Briefly Adds Alibaba, BYD and Other High-Profile Firms to List of Chinese Military Companies," Kharon Research, February 13, 2026, available at https://www.kharon.com/brief/us-china-news-alibaba-byd-defense-department-1260h .





(Source: https://x.com/Robo_Tuo/status/1991882471156457894)

This wide set of actors means that, although federal policy can and should target specific companies that are of concern to national security, a broader all-of-government strategic approach is needed to support the US robotics industry and to provide greater assurance of economic security.

Recommendations

We respectfully make the following recommendations to this subcommittee, to Congress, and to the broader United States government:

1. **Direct the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) to expeditiously undertake a national security evaluation of the use of foreign adversarial robots in American industry and governmental operations.**

Although private researchers have raised alarm by uncovering backdoors and vulnerabilities in specific Chinese robotics products on the market, these are one-off studies and we are not aware of any comprehensive government-led study of this issue. Such a study would provide clear guidance to private industry, government contractors, public safety agencies, and other stakeholders regarding the security of advanced robotics products acquired from foreign companies. The examination would be informative to both important end-users and policymakers and is, we believe, overdue.

2. Pass the *National Robotics Commission Act*, as a Step Towards a National Robotics Strategy

Recently, a bipartisan bill was introduced in the House that would establish a National Robotics Commission, H.R. 7334. Modeled on the AI and Biotech Commissions that were so useful to those industries and to government stakeholders, a Robotics Commission would bring experts, industry, and government together to recommend the policies that would support the growth and success of the industry.

Our company began calling for the development of a national robotics strategy in 2023. While Chinese advisory committees have already made quick progress on collaborative standards and strategies, and another five-year plan emerges from the Chinese government that elevates robotics even more than the prior plans, and while about a dozen other counties have their own robotics strategies, the United States government has yet to move forward with establishing a deliberative body or tasking an agency to begin developing its own national strategy. Time is running short and we urge Congress to move forward as soon as possible with this legislation and related policy efforts to kick-start the development of a national robotics strategy.

#

Boston Dynamics is grateful for the opportunity to share our perspectives with you on this important topic. I look forward to your questions.

TESTIMONY OF

Michael Robbins
President and Chief Executive Officer
Association for Uncrewed Vehicle Systems International (AUVSI)

BEFORE

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"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."

ON

March 17, 2026
Washington, DC

Introduction

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

My name is Michael Robbins, and I am the President and Chief Executive Officer of the Association for Uncrewed Vehicle Systems International, or AUVSI, the world's largest industry association representing robotics, uncrewed systems, and autonomous technologies. Our members develop and deploy advanced systems that operate in the air, on the ground, and in the maritime domain across commercial, public safety, and defense applications.

Advanced technologies can transform society for the better, improving safety, strengthening resilience, and expanding opportunity. However, these same technologies can also become a direct threat to freedom when serving authoritarian power. The technologies examined in today's hearing, particularly artificial intelligence systems and robotics platforms associated with companies based in the People's Republic of China (PRC) such as DeepSeek and Unitree Robotics, illustrate how emerging technologies can introduce new national security risks when developed within adversary-controlled technology ecosystems. Robotics systems of today are not simply software tools, nor are they the simple robots of the past executing a scripted task. They are networked machines capable of sensing, communicating, and acting in the physical world. When vulnerabilities exist in these systems, the consequences can extend beyond data exposure to surveillance, disruption of infrastructure, and physical operational risk.

While consumer-facing, 'chat-based' AI has attracted much of the public's attention, physical applications of AI-enabled robotics represent the next frontier. This integration of artificial intelligence technology in modern robotics and autonomous platforms allows for significant leaps in perception, navigation, and decision-making.

Here in the United States as well as among our allies, AUVSI's members, including Boston Dynamics, testifying with me here today, are at the leading edge of this transformation across the entire robotics technology stack. However, our adversaries – specifically the People's Republic of China – are methodically executing a centrally planned playbook to capture global market dominance at the direct expense of American industry**.** Backed by initiatives like "Made in China 2025" and fueled by over $137 billion in state investment funds, the PRC is deliberately flooding the global market with artificially cheap, subsidized robotic platforms. This aggressive dumping is designed to systematically undercut U.S. producers – offering systems at a fraction of the cost of American-made counterparts – which starves U.S. companies of the revenue needed to scale domestic industrial capacity and stifles private sector investment in research and development. Ultimately, this concerted national effort aims to hollow out the U.S. robotics industrial base, creating entrenched technological and industrial dependency while embedding structural cyber-physical vulnerabilities across our critical infrastructure.

This convergence between artificial intelligence and robotics is a major technological development. But it also introduces a new category of risk. When AI software systems are embedded in connected physical machines, the result is a cyber-physical system whose vulnerabilities can affect both digital networks and real-world operations. Furthermore, documented vulnerabilities and software backdoors, such as those in Unitree Robotics' Go1 robot and DJI's robot vacuums and drones, underscore how real this threat is: these vulnerabilities are not hypothetical, but a real and present threat to homeland security.[1] [2] [3]

Further underscoring the risk to U.S. national security, the PRC is aggressively weaponizing advanced civilian robotics to enhance its military capabilities, a reality that demands immediate Congressional attention. Recent footage released by the People's Liberation Army (PLA) starkly illustrates this threat, including a video ominously titled "The Robot Dog's Time to Kill Has Come," which depicts a Unitree Robotics quadruped equipped with an automatic rifle striking targets with precision. Chinese state media has broadcast joint military exercises featuring these robotic dogs operating alongside armed quadcopters and human troops in urban assault simulations, while recent university-led military training exercises have even deployed robot dogs capable of launching rockets.[4] To enable the autonomous navigation, terrain mapping, and off-road mobility of these platforms, the PLA frequently pairs these military robots with LiDAR sensors produced by subsidized Chinese firms, including Hesai, a company on the U.S. Department of Defense's 1260H designation as a Chinese military company, but still with deep penetration into the U.S. market.[5] This rapid battlefield integration is the direct result of Beijing's Military-Civil Fusion strategy, which systematically funnels ostensibly commercial technology through defense-linked universities into the hands of the PLA.

Crucially, the Chinese commercial robotics firms supplying these systems – such as Unitree – are bolstered by massive state subsidies and protective industrial policies deliberately designed to capture the global market at the direct expense of U.S. industry. By flooding the international market with artificially cheap robotic platforms, the PRC systematically undercuts American producers, starving U.S. companies of the revenue needed to invest in R&D and scale domestic industrial capacity. As these subsidized Chinese firms drive American competitors out of business, they are simultaneously functioning as critical research and development extensions of the PLA. As the PLA advances to the next phase of modern warfare by integrating artificial intelligence into these unmanned systems, we must recognize that allowing PRC dominance in the commercial robotics sector directly underwrites

[1] Sam Sabin, "Chinese Robotics Manufacturer Left Backdoor in Product," Axios, April 1, 2025, https://www.axios.com/2025/04/01/threat-spotlight-backdoor-in-chinese-robots-future-of-cybersecurity

[2] Eric Berger, "Spanish Engineer Reports Flaw in 'Smart' Vacuums After Gaining Control of 7,000 Devices," The Guardian, February 24, 2026, https://www.theguardian.com/world/2026/feb/24/spanish-engineer-smart-vacuums-remote-control

[3] Fortress Information Security, Securing the Skies: Case Study (v1.1), DJI Mini 2 Drone Teardown Exposes Security Risks, 2024, https://8759415.fs1.hubspotusercontent-na1.net/hubfs/8759415/Securing%20the%20Skies%20-%20Case%20Study_v1.1.pdf

[4] 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, https://www.kharon.com/brief/unitree-robotics-china-pla

[5] U.S. Department of Defense, "Notice of Designation of Chinese Military Company," Federal Register 89, no. 205 (October 23, 2024): 84547–84548, https://www.federalregister.gov/documents/2024/10/23/2024-24723/notice-of-designation-of-chinese-military-company

their military modernization, hollowing out U.S. industrial capacity and presenting a profound national security threat.

Unfortunately, we have seen this in the United States before in another segment of the autonomous systems industry. The PRC is executing the exact same centrally planned playbook in the advanced robotics sector that it used to decimate the U.S. commercial drone industry: leveraging massive state subsidies to flood the market with below-cost systems and deliberately drive American manufacturers out of business.[6] Propelled by initiatives like "Made in China 2025" and over $137 billion in state investment funds, subsidized Chinese robotics firms are artificially suppressing prices, starving U.S. companies of the revenue needed to scale domestic capacity, and maintain technological leadership.[7]

This aggressive economic market capture transforms into a dire national security threat when combined with the PRC's sweeping legal framework – including its National Intelligence, Cybersecurity, and Data Security laws – which legally compels all Chinese commercial entities to provide state intelligence services with unfettered access to their data and systems. Because modern robotic platforms are highly connected cyber-physical systems embedded across our logistics, manufacturing, and defense sectors, allowing PRC market dominance effectively installs Trojan horses, or embedded vulnerabilities, within U.S. critical infrastructure, exposing our nation to severe risks of data exfiltration, remote operational disruption, and the weaponization of our supply chains during times of conflict.

Furthermore, the systematic expropriation of U.S. technology extends beyond hardware into the very foundation of artificial intelligence through industrial-scale "distillation attacks". Leading Chinese AI laboratories – including DeepSeek, Moonshot, and MiniMax – are illicitly extracting the capabilities of advanced U.S. models to train their own systems.[8] By utilizing proxy networks and fraudulent accounts to farm millions of interactions from American models like Anthropic's Claude and OpenAI's ChatGPT, these PRC firms acquire frontier AI capabilities at a fraction of the time and cost required for independent development. This theft presents a severe and immediate national security risk: illicitly distilled Chinese models bypass the critical safety guardrails embedded in U.S. systems, directly enabling authoritarian governments to deploy frontier AI for offensive cyber operations, mass surveillance, and disinformation campaigns.

Furthermore, as highlighted by the Center for Strategic and International Studies, this accelerated development allows China to aggressively export its artificially cheap, open-weight models globally, securing future tech ecosystems in developing economies and fostering international dependence on

[6] Association for Uncrewed Vehicle Systems International (AUVSI), Partnership for Drone Competitiveness White Paper (Arlington, VA: AUVSI, 2025), https://www.auvsi.org/wp-content/uploads/2025/07/AUVSI-Partnership-for-Drone-Competitiveness-White-Paper.pdf

[7] 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

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

PRC technology.[9] DeepSeek is emblematic of how rapidly these capabilities can proliferate when illicit extraction, open weights, and state-driven incentives converge. When these unregulated, illicitly trained AI "brains" are combined with the heavily subsidized robotics platforms currently flooding the market, they create an unprecedented cyber-physical threat to U.S. national security and economic leadership.

We simply cannot allow this dangerous erosion of American industrial capacity and national security to happen, and AUVSI commends the Committee for holding this vital hearing to confront these urgent threats and ensure U.S. leadership in advanced robotics.

Recognizing both the critical importance of these technologies to the United States' economic competitiveness and national security, as well as the risks associated with insecure or adversary-linked systems, AUVSI recently launched our **Partnership for Robotics Competitiveness**, an industry initiative focused on strengthening U.S. leadership in robotics and physical artificial intelligence while addressing cybersecurity, supply chain, and national security risks associated with connected robotics systems.[10]

Robotics and Physical AI as a Homeland Security Issue

As AI-enabled robotics systems become more capable and more widely deployed, they are increasingly operating in highly sensitive environments with significant implications for homeland security. These include logistics hubs, ports, warehouses, manufacturing facilities, transportation systems, energy infrastructure, public safety operations, and emergency response environments.

In these settings, robotics systems are not isolated machines. They are connected cyber-physical platforms that combine sensors, software, networking, cloud connectivity, and physical actuation. They collect data from the surrounding environment, transmit and receive information across networks, and in many cases can be monitored, updated, or controlled remotely. That combination of digital connectivity and real-world physical action is what makes robotics in this context such a pressing homeland security issue.

That is what makes the risk posed here so significant: A compromised laptop exposes data; a compromised robot can expose data and move, map, surveil, disrupt operations, or create physical hazards. With advanced sensors used in these systems, including Light Detection and Ranging (LiDAR) sensors, the data exposed itself presents a unique risk: data vulnerabilities might mean a highly detailed three-dimensional map of critical infrastructure or other sensitive sites. Moreover, because these systems interface with the physical world, a compromised robot could present a physical threat in myriad ways:

[9] Richard Gray and Michael H. Gary, "Hedged Bets on the U.S.-China AI Race," Charting Geoeconomics (Center for Strategic and International Studies), January 20, 2026, https://www.csis.org/blogs/charting-geoeconomics/hedged-bets-us-china-ai-race.

[10] Association for Uncrewed Vehicle Systems International (AUVSI), Partnership for Robotics Competitiveness: Securing U.S. Leadership in Robotics and Physical Artificial Intelligence (Arlington, VA: AUVSI, 2026), https://www.auvsi.org/wp-content/uploads/2026/02/AUVSI-PFRC-Whitepaper.pdf.

creating safety hazards on jobsite, compromising public infrastructure, and allowing our adversaries persistent access into a broader operational environment from the battlefield to the factory floor.

Cyber-Physical Risk in Connected Robotics Systems

Modern robotics systems should be understood as connected cyber-physical platforms that combine software, communications networks, sensors, and physical machines capable of interacting directly with real-world environments. As these systems become more advanced, they increasingly rely on cloud connectivity, remote monitoring, over-the-air software updates, and continuous data collection to support performance improvements, predictive maintenance, and adaptive learning. While these capabilities provide important operational benefits, they also expand the attack surface associated with robotics systems and introduce new forms of cyber-physical risk.

In practical terms, these risks generally fall into three categories:

- First, robotics systems create data exposure risks. Connected robots routinely collect detailed operational data from the environments in which they operate. This can include facility layouts, movement patterns, environmental sensing data, workflow information, and records of human–machine interaction. Over time, aggregated data from these systems can reveal sensitive insights about infrastructure operations, logistics networks, and industrial processes.
- Second, robotics platforms create remote disruption risks. If vulnerabilities exist in software, firmware, communications links, or cloud management tools, these systems may be susceptible to unauthorized observation, manipulation, or loss of control. Because robotics platforms operate in the physical world, a cyber compromise can translate directly into physical consequences, including disruption of operations or interference with safety-critical environments.
- Third, connected robotics systems can create persistent access risks through update and support pathways. Many systems rely on remote software updates, cloud services, and vendor-managed diagnostics throughout their lifecycle. When those pathways remain accessible after deployment, they can create long-term dependencies on external software environments and provide ongoing access points into operational systems.

Recent incidents illustrate these risks in concrete terms. Security researchers identified an undocumented access pathway in a Unitree Go1 quadruped robot that allowed remote access to camera feeds and control functions without user authorization, demonstrating how hidden vulnerabilities in connected robotics platforms can enable both surveillance and system takeover.[11]

The potential implications of these technologies have also drawn bipartisan concern in Congress. In 2025, members of the House Select Committee on the Chinese Communist Party warned that robotics platforms, such as those produced by Unitree, could present surveillance and national security risks if deployed within sensitive U.S. institutions and infrastructure environments. The Committee also urged

[11] Dave Lawler, "Threat Spotlight: Backdoor Found in Chinese Robots," *Axios*, April 1, 2025, https://www.axios.com/2025/04/01/threat-spotlight-backdoor-in-chinese-robots-future-of-cybersecurity.

that Unitree be accordingly designated as Chinese Military Companies under 1260H of the FY2021 National Defense Authorization Act.[12] It is notable that when the Department of Defense briefly updated the 1260H list in February of 2026, Unitree Robotics was listed, however the list was rapidly taken down after posting.

Sensor Risk, LiDAR, and Sensitive Infrastructure Mapping

Modern robotics and autonomous systems rely on integrated sensing suites that may include cameras, radar, and LiDAR to perceive and navigate their environments. These sensing technologies allow machines to identify obstacles, understand spatial relationships, and operate safely alongside people and other equipment.

Among these technologies, LiDAR merits particular attention because of its ability to generate high-resolution, three-dimensional representations of physical environments. In robotics and autonomous systems, LiDAR supports localization, mapping, obstacle detection, and coordinated autonomous behavior. These capabilities allow robotic systems to move through complex environments, build detailed maps of their surroundings, and perform tasks with increasing levels of autonomy.[13]

However, the same capabilities that make LiDAR valuable for robotics applications can also introduce security concerns when deployed in sensitive environments. It is almost certainly for this reason that a LiDAR sensor was used by Chinese intelligence in an attempt to map a U.S. military installation in the Philippines.[14]

Because LiDAR sensors continuously generate precise spatial data, they can produce highly accurate digital maps of the environments in which they operate. In industrial or infrastructure settings, this may include facility layouts, equipment locations, operational workflows, and patterns of movement within a site. Over time, aggregated data from these sensors can provide detailed insight into how facilities function and how sensitive environments are structured.

Where LiDAR-enabled systems are deployed in factories, ports, logistics hubs, transportation nodes, energy infrastructure, warehouses, or public safety environments, they can generate persistent spatial

[12] U.S. House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, “Trojan Horse Tech: Select Committee Sounds Alarm on CCP Robots Inside U.S. Institutions,” press release, May 7, 2025, https://chinaselectcommittee.house.gov/media/press-releases/trojan-horse-tech-select-committee-sounds-alarm-on-ccp-robots-inside-us-institutions.

[13] Association for Uncrewed Vehicle Systems International (AUVSI), *Partnership for Robotics Competitiveness: Securing U.S. Leadership in Robotics and Physical Artificial Intelligence* (Arlington, VA: AUVSI, 2026), https://www.auvsi.org/wp-content/uploads/2026/02/AUVSI-PFRC-Whitepaper.pdf.

[14] 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, https://www.fdd.org/analysis/2025/02/03/philippines-busts-chinese-spy-ring-targeting-u-s-and-allied-military-infrastructure/

awareness of locations that may be commercially sensitive, operationally sensitive, or nationally sensitive.[15]

These concerns are not hypothetical. In June 2025, AUVSI wrote to New York state and city officials warning about potential security risks associated with LiDAR sensors manufactured by Livox, a Chinese company owned by DJI, after such sensors were observed deployed at JFK International Airport and Penn Station in New York City.[16]

As described in that letter, LiDAR sensors can collect detailed real-time spatial data that could reveal sensitive information about transportation infrastructure, security postures, and crowd flow patterns if compromised or accessed by adversaries. In this case, these sensors were deployed in a static setting, affixed to certain points at these facilities; deployed in a dynamic setting, such as on a robotic platform, further compounds the threat.

Structural and Jurisdictional Risk in Networked Robotics Systems

Cyber-physical risk in robotics systems cannot be evaluated solely through the lens of individual software vulnerabilities or hardware components. Instead, these risks must be understood within a broader geopolitical and legal context of supply chains, software dependencies, and data flows.

Modern robotics platforms are not standalone machines. They are networked cyber-physical systems that often rely on cloud services, data streams, remote diagnostics, and software updates delivered throughout the operational life of the system. These features provide important operational benefits but also create ongoing connections between deployed machines and the vendors responsible for maintaining them, such as ongoing software and firmware updates, data storage, and even remote access.

Accordingly, China's legal and regulatory framework governing technology companies must be considered when evaluating the security implications of connected robotics platforms. Unitree Robotics and DeepSeek, like any Chinese company, operate within the legal system of the People's Republic of China. Under China's national security laws, these companies can be, and are, compelled to operate functionally as an instrument of Chinese Communist Party (CCP).[17] [18]

[15] Foundation for Defense of Democracies Action, "Policy Alert: Urgent U.S. Response Needed to Counter China's Strategic Use of LiDAR Technology," September 23, 2025, https://www.fdd.org/analysis/2025/09/23/urgent-us-response-needed-to-counter-chinas-strategic-use-of-lidar-technology/.

[16] Association for Uncrewed Vehicle Systems International (AUVSI), Letter Regarding Security Risks of Livox LiDAR Deployments at JFK Airport and Penn Station, March 2026, https://www.auvsi.org/wp-content/uploads/2026/03/AUVSI-Livox_JFK_PennStation.pdf

[17] Chun Han Wong, "China Adopts Sweeping National Security Law," The Wall Street Journal, July 1, 2015, https://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589

[18] Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI), Cybersecurity Guidance: Chinese-Manufactured Unmanned Aircraft Systems (UAS), January 17, 2024, https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf

A series of national security and data governance laws, including the National Intelligence Law, Cybersecurity Law, Data Security Law, and Personal Information Protection Law, collectively establish an environment in which companies operating within China's technology sector may be required to cooperate with state intelligence and security authorities and provide access to relevant data, systems, or technical capabilities.[19] The National Intelligence Law mandates that all citizens and organizations must assist and cooperate with national intelligence work when requested. This provision establishes a legal obligation for companies to comply with intelligence-related directives issued by state authorities whatever they may be. This is further entrenched by China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law which establish mechanisms through which government authorities may require access to data, technical systems, or other information under the control of companies operating within China's technology ecosystem.

These legal obligations create structural pathways through which operational data or system access could become available to the Chinese state. As a result, risks associated with connected robotics platforms are not limited to technical vulnerabilities alone; they are also shaped by the legal jurisdiction governing the companies that design, manufacture, and maintain those systems. In this case, the laws promulgated by the CCP. In the context of connected robotics systems, where cloud services, telemetry data, remote diagnostics, software updates, and continuous data collection are core operational features, these authorities create structural pathways through which operational data or system access could be obtained by the state.

Cyber-physical risk exposure in robotics systems is not neutral across suppliers but rather is greatly shaped by the legal framework governing the companies that develop, maintain, and support the technology. Accordingly, the risks posed here are not normal cybersecurity risks but rather a potential vector for nation state-level cyber warfare enabled by Chinese law and civil-military fusion. Knowing this, it is therefore crucial that policy action be taken to address the serious and unique threat posed by PRC-based companies across the entire robotics technology stack.

Economic Competition and Supply-Chain Risk in Robotics

Beyond cybersecurity considerations, robotics must also be understood through the lens of global economic competition and industrial policy. Advanced robotics systems depend on complex supply chains that include rare-earth magnets, electric motors, batteries, precision actuators, sensors, semiconductors, and specialized software systems. These components are deeply integrated into robotics platforms and are not easily interchangeable.

Over the past two decades, the People's Republic of China has pursued a coordinated national strategy to build dominance across many of these enabling technologies. Through unprecedented subsidies, preferential financing, industrial planning, and coordinated investment, Chinese firms have rapidly

[19] Association for Uncrewed Vehicle Systems International (AUVSI), *Partnership for Robotics Competitiveness: Securing U.S. Leadership in Robotics and Physical Artificial Intelligence* (Arlington, VA: AUVSI, 2026), https://www.auvsi.org/wp-content/uploads/2026/02/AUVSI-PFRC-Whitepaper.pdf.

expanded production capacity across multiple layers of the robotics technology stack. At the national level, China's top economic planning agency announced a ¥1 trillion yuan (roughly $137 billion) venture capital fund dedicated to robotics, artificial intelligence, and advanced technologies. This is compounded at the local level by municipal governments and state-backed hedge funds, including a $14 billion robotics and AI fund in Beijing and a $77 million embodied AI fund in Shanghai. Furthermore, China's government-controlled banks have increased industrial lending by a staggering $1.9 trillion over the past four years to bankroll factory construction and robotic automation.[20]

These efforts are closely tied to China's Military-Civil Fusion strategy, which explicitly seeks to integrate civilian technological innovation with national defense and intelligence objectives. State-backed firms operating with this massive, multi-tiered financial backing can aggressively dump products at artificially suppressed prices, placing market-based American companies at a severe structural disadvantage.

Over time, this deliberate strategy leads to market capture, supply-chain concentration, and dangerous technological dependency. We have seen this exact centrally planned playbook executed before in the commercial drone industry, where sustained dumping by heavily subsidized Chinese firms like DJI decimated the U.S. drone manufacturing base and left our nation dangerously dependent on adversary-linked technology.

Fortunately, we still have a critical window of opportunity to stop this from happening to the robotics industry. However, if we fail to act before PRC market dominance hardens into structural dependence, U.S. and allied companies will be forced out of the global market by these unfair trade practices, leading to the widespread deployment of unsecure robotic systems that amount to a global backdoor into our critical infrastructure.

Policy Steps Congress Can Take Now

As robotics and autonomous systems become increasingly embedded in infrastructure, logistics, manufacturing, and public safety environments, policymakers must consider how these technologies intersect with cybersecurity, supply chain integrity, and infrastructure protection.

Accordingly, AUVSI urges Congress to consider several policy priorities:

- **Congress should support the development of a coordinated national strategy for robotics and physical artificial intelligence.** Robotics is rapidly becoming foundational infrastructure for modern economies and future military operations, yet the United States lacks a comprehensive federal strategy guiding policy across research, manufacturing, deployment, workforce development, and supply chain security. Bipartisan legislation introduced this Congress, such as the ***National Robotics Commission Act*** *(H.R. 7334)*, introduced by Congressman Jay Obernolte (CA-23) and Congresswoman Jennifer McClellan (VA-03), would take crucial steps towards a

[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

national strategy by working to align federal efforts, set measurable goals, and ensure sustained U.S. leadership in this strategically important technology domain.

- Leadership in advanced robotics is essential for **sustaining the American workforce**. Rather than replacing human labor, robotics augment our workforce, addressing persistent labor shortages, improving occupational safety by taking over hazardous tasks, and keeping U.S. manufacturing globally competitive. **AUVSI explicitly calls for a comprehensive National Robotics Strategy that prioritizes robust workforce development programs.** By pairing these initiatives with workforce development tax credits, we can offset the costs of training workers for the robotics age, transitioning the American workforce toward higher-skilled programming, system integration, and maintenance roles that command higher wages.
- **Congress should build on recent work addressing adversary-linked uncrewed ground vehicles, including robotics, in federal procurement.** AUVSI was active in supporting the inclusion of a provision in House version of the FY 2026 National Defense Authorization Act which would have prohibited federal procurement of uncrewed ground vehicles produced by foreign countries of concern, such as the PRC. This would have restricted government procurement of any uncrewed ground system – from small multipurpose robots to large autonomous vehicles. Beyond managing the serious risks posed by deployment of these systems by the federal government, federal procurement policies play a powerful role in shaping emerging technology markets. Accordingly, we urge Congress to take up this measure again as a standalone bill as well as in this year's National Defense Authorization Act.
- **Congress should continue advancing risk-based restrictions on adversary-linked technologies deployed in infrastructure environments.** Legislation such as the ***Securing Infrastructure from Adversaries Act*** *(H.R. 4802 / S. 4000)* reflects serious risks posed by foreign-adversary made LiDAR sensors embedded within sensitive operational environments. Robotics systems, sensors, and related technologies produced within adversary-controlled ecosystems introduce surveillance vulnerabilities, data exposure risks, and persistent access pathways into critical infrastructure systems. Establishing clear authorities to evaluate and restrict the deployment of adversary-linked technologies in critical infrastructure environments represents an important step toward protecting the security and integrity of the nation's operational systems.
- **Policymakers should continue examining the security implications of key enabling technologies used in robotics and autonomous systems**. Technologies such as advanced sensing systems, including LiDAR, are foundational to the operation of modern robotics platforms. At the same time, their ability to generate detailed spatial and environmental data raises important security considerations when deployed in sensitive environments. The ***SAFE LiDAR Act*** *(H.R. 6576)* represents an important effort to address these risks by evaluating the national security implications associated with certain LiDAR technologies and by promoting greater transparency into the supply chains behind these systems. Beyond this, we urge Congress to consider similar measures across the robotics technology stack.

- Addressing the cyber-physical risks requires not only restricting unsafe technologies but also accelerating the growth of trusted alternatives. **Congress should prioritize strengthening the U.S. robotics industrial base and building secure allied supply chains for critical technologies.** Congress should support policies that expand U.S. robotics manufacturing, use federal procurement and demand signals to support trusted systems, and encourage private investment in domestic production to build resilient supply chains for critical robotics components; including sensors, batteries, rare earth magnets, and advanced electronics.

Taken together, these efforts represent important early steps toward developing a broader policy framework for addressing cyber-physical risk in robotics and autonomous systems. By proactively addressing these issues now, Congress can help ensure that robotics technologies strengthen U.S. infrastructure, economic competitiveness, and national security rather than introducing new vulnerabilities into the systems that underpin the nation's economy and public safety operations.

Conclusion

The issues raised by companies such as DeepSeek and Unitree Robotics reflect a broader challenge as robotics, artificial intelligence, and autonomous systems become increasingly embedded across the U.S. economy and critical infrastructure. These technologies are rapidly becoming foundational to logistics networks, manufacturing systems, transportation infrastructure, energy operations, and public safety environments. While they offer significant benefits in productivity, efficiency, and safety, their growing integration into the physical world also means that vulnerabilities in these systems, or in the ecosystems that produce them, can introduce serious risks to both national security and economic resilience.

The threat posed by PRC-linked robotics companies must be understood within this broader context. These firms operate within a state-directed system that combines aggressive industrial policy, supply-chain consolidation, and legal obligations to cooperate with state intelligence authorities. When robotics platforms produced within this ecosystem are deployed in sensitive environments, the risks extend beyond ordinary cybersecurity concerns to include potential surveillance, exposure of sensitive operational data, and persistent access to critical infrastructure systems. At the same time, sustained subsidies and coordinated industrial strategies can enable these companies to capture global markets, creating technological dependencies that are difficult to reverse once systems are widely deployed.

For the United States, the challenge is therefore both a security issue and a strategic economic one. Ensuring that robotics systems deployed across our infrastructure and industries are secure, trusted, and developed within resilient supply chains will be essential to protecting both national security and long-term technological leadership. By recognizing the strategic implications of robotics and taking proactive steps to address the risks posed by adversary-linked technologies, Congress can help ensure that the next generation of robotics strengthens, rather than undermines, the security, resilience, and competitiveness of the United States. AUVSI and our members stand ready to work with Congress and federal agencies to support that effort.

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.