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.