TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Judiciary Committee

Embedded Threats: Foreign Ownership, Hidden Hardware, and Licensing Failures in America's Transportation Systems

EMILY DE LA BRUYÈRE

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
January 21, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Chair Van Drew, Ranking Member Crockett, thank you for the opportunity to testify today.

The Chinese Communist Party (CCP) wants to control global resources, markets, and data — so that it can control global prosperity, security, and information. Beijing pursues this ambition by leveraging non-market industrial policy through which it subverts critical supply chains and networks; a strategy of "military-civil fusion" through which it converts that civilian positioning into a forward-deployed military presence; and a state-sponsored program of data collection and aggregation through which every Chinese company, component, and platform becomes positioned for espionage and influence.

Transportation systems are a core part of this Chinese strategy. Transportation systems encompass vehicles themselves, whether rail cars or autonomous cars; the infrastructure on and through which they operate, such as toll systems and bridges; and the components and platforms that power them, ranging from in-car artificial intelligence (AI) agents to semiconductors to LiDar.

China's Framing and Threat

Transportation systems fall within Beijing's framing of the "military-civil fusion" ecosystem. They enable social functioning, industrial operation, and military mobilization. China therefore both protects them domestically and seeks to penetrate them internationally.[1]

Transportation systems also represent a massive economic opportunity. These are industries of industries. Their markets are enormous. So are those of the industries they drive, like rubber for tires, sensors for toll systems, and aluminum for capacitators. Across the board, the relevant industrial and technological capacity has direct military applications; it generates security as well as economic rewards. Beijing therefore wants to capture global transportation markets, supply chains, and industrial and technological capacity. And Beijing wants to do so at the expense of its rivals, namely the United States.

Modern technological trends both generate a unique opportunity for Beijing to succeed and raise the stakes of such success. The intelligent, connected era is revolutionizing transportation. This creates an opening for a disruptor — China — to upset incumbents in the sector, the United States and the West. Beijing is rapidly securing dominance over emergent inputs into modern transportation systems. These include components like semiconductors and sensors, software and transportation platforms, and vehicles themselves, whether smart cars or electric buses. In many cases Beijing is doing so without broad recognition of its menace — because of its incremental

[1] See, for example, the "军民融合发展战略纲要 [Outline of the Strategy for Integrated Military and Civilian Development]," issued by the Central Commission for Integrated Military and Civilian Development in 2018; Annie Fixler, RADM (Ret.) Mark Mongomery, and Rory Lane, "CSC 2.0: Military Mobility Depends on Secure Critical Infrastructure," *Foundation for Defense of Democracies*, March 27, 2025. (https://cybersolarium.org/csc-2-0-reports/military-mobility-depends-on-secure-critical-infrastructure)

approach and because, capitalizing on a new technological paradigm, Beijing is playing a different game than incumbents in the sector.

Perhaps most importantly, today's technological revolution means that every foothold in the transportation sector — every component, software system, and vehicle — is a strategic as well as an economic asset; a possible back door to collect, disrupt, and shape information. Everything is a computer. China is hacking all of it.

China's efforts to co-opt U.S. and global transportation systems, therefore, do not only create supply chain and market risks, threatening the autonomy and economic rewards that come from industrial capacity. China's subversion also grants Beijing access to critical information on American society; the ability to influence that information; and the power to destabilize foundational systems on which American society depends.

The State of Play

This is not a notional danger. China's presence is already well advanced. The United States is already under attack.

Take, for instance, LiDar.[2] LiDar is used by autonomous vehicles to map their surroundings, by airports to track movement and crowds, by toll systems to detect vehicles, and by road and bridge operators to scan for defects. Thanks to non-market support, including subsidies and backing from the military-civil fusion apparatus, Chinese companies dominate the sector: They claim more than 93 percent of the global automotive LiDar market and almost 90 percent of the total LiDar market.[3]

Among China's leading LiDar champions are companies — like Hesai Technology, Huawei, and DJI — that the U.S. government has identified as Chinese military companies. The Pentagon recently concluded that another top Chinese LiDar company, Robosense, also merits inclusion on the Pentagon's 1260H list of military-linked Chinese companies.[4] Hesai supplies Amazon's Zoox, Aurora Innovation, General Motors's Cruise, and Nvidia's Drive Hyperion.[5] Hesai's LiDar sensors are used at the Charlotte Douglas International Airport and Portland International Airport — and have been installed at intersections in Chattanooga, Tennessee, and on drawbridges in Sarasota, Florida. LiDar sensors from DJI's LiDar subsidiary Livox have been deployed in major

[2] LiDar is a remote sensing technology that uses pulsed laser light to measure distances.
[3] "China takes the lead in automotive LiDAR: A market set to quadruple by 2030," *Yole Group*, June 24, 2025. (https://www.yolegroup.com/press-release/china-takes-the-lead-in-automotive-lidar-a-market-set-to-quadruple-by-2030)
[4] "Pentagon seeks to add Alibaba, Baidu, BYD to China military list, Bloomberg News reports," *Reuters*, November 26, 2025. (https://www.reuters.com/world/china/pentagon-suggests-adding-alibaba-baidu-byd-list-aiding-china-military-bloomberg-2025-11-26)
[5] Daniel Ren, "Nvidia chooses China's Hesai for lidar sensors in Hyperion autonomous driving platform," *South China Morning Post*, January 6, 2026. (https://www.scmp.com/business/china-business/article/3338909/nvidia-chooses-chinas-hesai-lidar-sensors-hyperion-autonomous-driving-platform)

American transit hubs ranging from Moynihan Hall/Penn Station to JFK International Airport.[6] RoboSense supplies Lucid Motors and Rivian. Dallas Fort Worth International Airport in 2025 announced that it would procure Robosense LiDar.[7]

Every purchase of a Chinese LiDar sensor funds the Chinese Communist Party. Every Chinese LiDar sensor — whether in electronic tolling systems, autonomous vehicles, or airports — risks collecting information for Beijing. And all could be turned off at China's command.[8]

A similar story holds across the larger ecosystem of components that power intelligent transportation. Internet of Things (IoT) modules enable fleet management and IoT-based tolling. China is the world's largest player in that market — thanks to companies that the U.S. government has identified as Chinese military companies like Quectel and China Mobile.[9] Optical transceivers support traffic signal control networks; railway, highway, and airport communication systems; and in-vehicle communication among cameras, radar, LiDar, and ultrasonic sensors.[10] China's Innolight alone holds more than 10 percent of the global market for optical transceivers.[11] Also in the list of top companies are China's Accelink, China's Huawei Hisilicon, and China's Eptolink.

Like LiDar, these components collect data, are vulnerable to attack, and are essential inputs into not only transportation systems but also data, communication, and computing infrastructure. As with LiDar, Beijing is deliberately securing a stranglehold over their global markets. And as with LiDar, the U.S. transportation ecosystem is embedded with them.

Increasingly, Beijing is also developing the platform level for modern transportation systems. This includes in-car software systems, ranging from legacy navigation software, like AutoNavi, to emergent, AI in-car agents like Simo, developed by a joint venture between Geely and Baidu. China's platform positioning also includes global smart shipping and supply chain networks like Alibaba's Cainiao and logistics solutions like China's National Transportation Logistics Platform

---

[6] "Comments on 'Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles' Proposed Rule," *Coalition for Safe and Secure Technology*, April 30, 2024. (https://secureenergy.org/safes-coalition-for-reimagined-mobilitys-comments-on-the-department-of-commerces-securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles-notic)

[7] Anne-Sophie Dubois, "Dallas Fort Worth Airport Selects Outsight for the World's Largest 3D LiDAR Deployment," *Outsight*, December 15, 2025. (https://insights.outsight.ai/dallas-fort-worth-airport-selects-outsight)

[8] RADM (Ret.) Mark Montgomery, "Lidar: Another emerging technology brought to you by China," *Defense News*, April 25, 2024. (https://www.defensenews.com/opinion/2024/04/25/lidar-another-emerging-technology-brought-to-you-by-china); Craig Singleton and RADM (ret.) Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," Foundation for the Defense of Democracies, December 2, 2024. (https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems)

[9] Charles Parton, "Chinese cellular (IoT) modules: Countering the threat," *Council on Geostrategy*, March 19, 2024. (https://www.geostrategy.org.uk/research/chinese-cellular-iot-modules-countering-the-threat)

[10] Optical transceivers are interconnected components that can transmit and receive data.

[11] "Top Optical Transceiver Manufacturers List (2024)," *Optcore*, June 26, 2024. (https://www.optcore.net/article056/?srsltid=AfmBOoqZqoVdbqUd58RmiFSrAhglPBuBCAeGGsbIPDyNFFQPWSyM4BZQ)

(LOGINK). LOGINK provides a centralized window into the otherwise fragmented world of global shipping, under the Chinese government's control.[12] Like China's component-level footholds in transportation systems, these platforms grant the Chinese Communist Party access to information and the ability to disrupt international movement. These platforms also empower Beijing to *shape* that information, the movement it defines, and the markets built on top of it.

China's presence, at a component and a platform level, in American transportation systems grants Beijing the power to turn off U.S. infrastructure. But even short of such an attack, China's footholds, already and constantly, allow the Chinese Communist Party to collect data on Americans that threatens citizens' privacy and the country's competitiveness. As I speak, Beijing is monitoring which Americans are moving where. In doing so, Beijing collects large-scale data on American society. That data amounts to a strategic asset.

China's presence in transportation systems also attacks the U.S. industrial base. Beijing uses its footholds in supply chains to move up the value chain — from, for example, car parts to car modules to car software to cars themselves. Beijing accomplishes this through non-market and illicit means, like forced tech transfer and intellectual property theft. Beijing also does so through entirely licit avenues, like the collaboration of U.S. and international champions desperate for access to China's market, production, and expertise.

As China moves up the value chain, its threat to transportation systems, and therefore to America, becomes both more firmly embedded and larger. The information that a single software system in a car collects pales next to that gathered by the car as a whole.[13] The consequences of a LiDar sensor being deactivated pale next to those of entire fleets of vehicles being turned off.

In addition, the growing sophistication of China's industrial offensive in the transportation sector attacks the heart of U.S. industry — including the defense industrial base. If China subverts the global auto industry, America will lose some 11 million jobs and 1.2 trillion dollars in output.[14] If China subverts the aviation industry, the U.S. will lose some 1 million jobs and $250 billion in output.[15] Those figures represent our sovereign industrial base. Losing those jobs and dollars will mean losing the industrial and technological capacity needed to sustain America's military and innovate for our security.

---

[12] "China's National Transportation Logistics Project," *Horizon Advisory*, August 2021. (https://www.horizonadvisory.org/geopolitical-operating-system)
[13] Elaine K. Dezenski, "Trojan Horse: China's Auto Threat to America," Testimony before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party, December 11, 2025. (https://www.fdd.org/wp-content/uploads/2025/12/Elaine-Dezenski-Testimony-12.11.25.pdf)
[14] "Alliance for Automotive Innovation Releases NEW Economic Data," *Alliance for Automotive Innovation*, January 29, 2025. (https://www.autosinnovate.org/posts/press-release/auto-innovators-data-driven-report-release)
[15] Brianna Wilson, "Understanding the Leadership Position of U.S. Aviation Manufacturing," *Monitor Daily*, February 4, 2025. (https://www.monitordaily.com/understanding-the-leadership-position-of-u-s-aviation-manufacturing)

This is a near threat. Thanks to its dominance at the upstream of the supply chain, its dedicated industrial and technology strategy, and the willingness of U.S. and international champions to hand over research and development, China's auto champions are increasingly the world's. BYD — one of China's most heavily subsidized companies — overtook Tesla in 2025 to become the world's largest EV seller. The average price of a BYD vehicle is about $17,000, compared to about $40,000 for a new Tesla. The same story risks playing out in the aviation industry. In no small part due to its partnerships with Airbus, China's state-owned COMAC is directly challenging that company and Boeing with its C919.[16]

What To Do: A Path Forward

China's ambitions in the transportation sector, and the corresponding danger to the United States, are not new. They date back more than a decade. But the situation is newly urgent. The sector is at a tipping point. Without action, America will sacrifice security, prosperity, and freedom.

But action is possible.

The first step is to stop further Chinese penetration of transportation systems; to protect critical U.S. infrastructure from Huaweis and hidden Huaweis. Washington should prohibit any transportation system or company that incorporates components or software made by Chinese or Chinese-influenced companies from receiving federal dollars, tax credits, or other incentives.

In the process, Washington should tighten the definition of what it means to be a Chinese or Chinese-influenced company. That definition should build on the U.S. Commerce Department's framing of a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." The definition should cover any company that is owned or invested in by Chinese entities; is under Chinese jurisdiction; has a tech licensing deal with a Chinese entity; localizes data, research, development, or production in China; or that invests in Chinese entities. This ban and definition should be both strictly framed and strictly enforced to protect against Chinese circumvention, localization, and other means of evasion. Prohibited Foreign Entity (PFE) and Foreign Entity of Concern (FEOC) rules provide an immediate opportunity to implement and scale such restrictions across sectors, including transportation.

These targeted measures can catalyze immediate change in and send a signal about China's presence in American transportation systems. But Washington must also take broader action to change the fundamental state of play that has allowed Beijing to secure its current footholds across America's critical infrastructure.

That action starts with protecting the U.S. market from China. Higher tariffs on Chinese goods can help to neutralize the non-market industrial offensive through which Beijing distorts markets

[16] Stuart Lau, "EU Champion Airbus has deep links to Chinese military industrial complex, report says," *Politico*, June 22, 2022. (https://www.politico.eu/article/eu-champion-airbus-has-deep-links-to-chinese-military-industrial-complex-report-says)

and co-opts supply chains. Such tariffs can dissuade the U.S. private sector from purchasing Chinese products and thereby becoming complicit with Beijing's industrial offensive. Tariffs also provide the conditions necessary to rebuild the domestic industry that the CCP has decimated.

In parallel, Washington can also protect American data — with it, the privacy of Americans and the country's competitiveness. No company that stores data in China should be permitted to collect data in the United States, or be eligible for federal procurement, federal tax credits or other incentives, or defense-industrial base procurement.

Washington must activate the U.S. private sector. Extant business models effectively hinge on forfeiting valuable U.S. technologies and positioning to China — and reject proactive investments in domestic industry. Washington can change that. The American private sector should have to choose between the U.S. and Chinese markets. Washington should prohibit any Chinese company, as well as any company that leverages components from, has a tech licensing deal with, has investment from, or has a joint venture with a Chinese company, from defense-industrial base procurement, federal procurement, or federal tax credits.

The U.S. must also recognize that the U.S.-China competition is not a bilateral one. China's presence is global. Defending against it requires a global approach. Washington should leverage trade deals, including a reauthorized USMCA, to compel American allies and partners, and American allied and partner private sectors, to implement their own protections against China, rather than serving as conduits for the Chinese Communist Party to establish oversea beachheads and access to the United States.

All of these measures are sticks. There are carrots for Washington to offer, too. Removing China from the American market broadly, and the transportation sector specifically, will incur short-term costs. It is up to Washington to ensure that, after decades of decimation at Beijing's hands, U.S. industry has the conditions necessary to succeed; and that investment, commercialization, and production in the United States are possible and potentially profitable. Washington should provide the infrastructure necessary for production, including through the expanded provision of domestic and upstream resources, a permissive regulatory environment, and a skilled workforce. And Washington should provide incentives for trusted companies and solutions to replace China's in American transportation infrastructure.

America has a chance to reindustrialize and renew — and, in the process, to restore national security. The transportation sector should be core to that effort. It might seem impossible now to think that China could supplant American giants like Ford, Boeing, and FedEx. But that scenario is on the horizon. And the industrial and technological capacity, supply chain leverage, data advantage, and coercive power that Beijing is positioned to capture through its transportation subversion will help the Chinese Communist Party win out more broadly. Washington must fight back.