April 30, 2026

Dr. Chris Miller
Nonresident Senior Fellow, American Enterprise Institute
Professor, The Fletcher School, Tufts University

Testimony before the U.S.-China Economic and Security Review Commission

Taking a Bigger Byte: China's Expanding Strategy for Data Dominance

Introduction

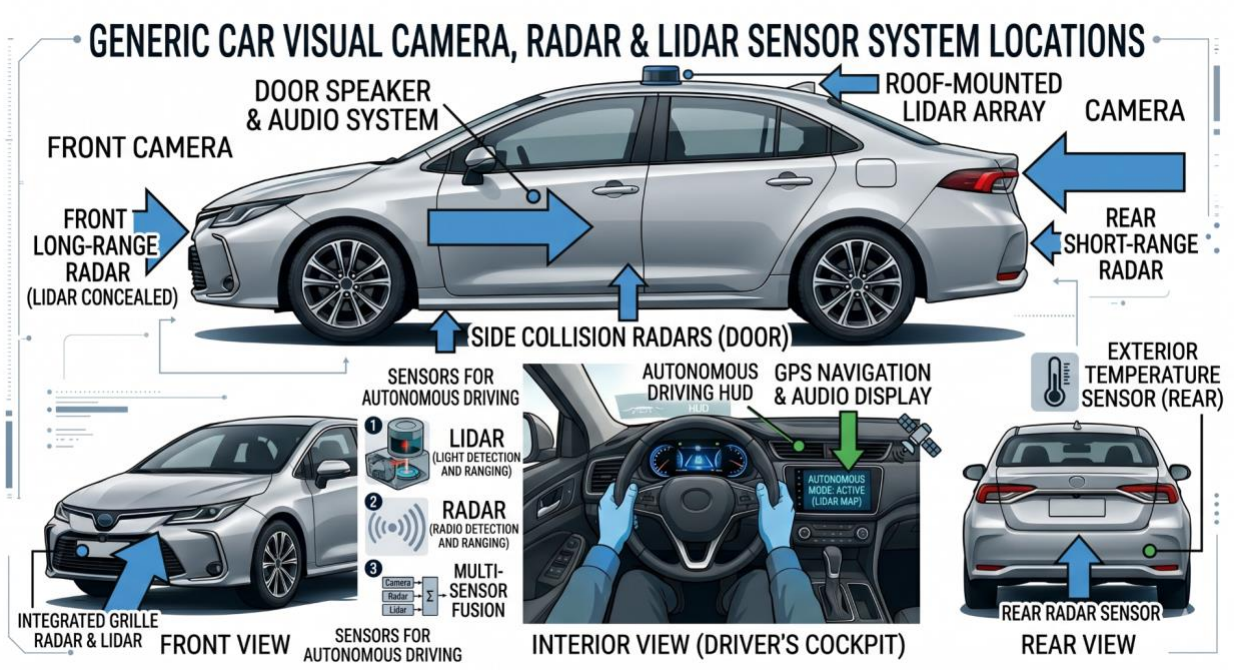
Packed with sensors, connected to the internet, and controlled by complex and opaque layers of software, modern cars represent a significant data collection and cybersecurity risk. Every generation of car gathers more data about its passengers and the outside world. Increasingly autonomous driving requires acquiring camera and lidar data about America's streets. Meanwhile, China has become the world's largest car producer and a leader in certain automotive technologies. Chinese-made cars have surged into the auto markets in allied countries. Though Chinese cars are relatively rare in the U.S., Chinese components have surged into U.S. automotive supply chains.

Use of Chinese software, connectivity systems, and critical components in autos creates significant risks, both of espionage and–in a potential future military crisis–of sabotage. The U.S. government has restricted use of Chinese-origin components for auto connectivity systems and has also limited use of Chinese code in certain types of auto software. However, some U.S. auto companies are pushing to relax these rules to allow closer partnerships with Chinese firms–and thus greater use of Chinese technology in American cars.

Properly calibrating restrictions on use of Chinese components in U.S. cars is important to the automotive and mobility industry. The race toward increasingly autonomous driving will have dramatic economic implications and will also raise substantial cyber security concerns. The U.S. government's posture toward Chinese components in connected cars will also set the tone for future regulation–or lack thereof–of other types of physical AI and robotic systems. As autonomous driving systems improve, as China's auto and auto component exports surge, and AI enables new types of robotics systems, Congress faces an important moment to mitigate risk of reliance on Chinese critical components in our cars.

I. Automotive Sensors, Privacy, and Intelligence Gathering

Fig. 1: Generic Example of Common Sensor Systems in a Car[1]



Modern cars have dozens of sensors that collect data about the car and its environment. This represents a major change for the auto industry: until relatively recently, most cars had only a handful of sensors, which generally assessed the internal operations of the car, especially the engine. Today, even many of these internally-focused sensors transmit data, with even some tire pressure gauges connecting to the cloud. Yet the biggest change is the dramatic increase in the number of sensors examining the external environment or collecting information about the driver. There are three key categories of sensor that raise intelligence collection concerns.

A. Location Sensors

Today, nearly every car connects to GPS. Location data–especially location data for cars driven by government employees–is a useful dataset for foreign intelligence services. For example, the location to which a person commutes daily provides strong evidence about which organization they work for.

B. Sensors Inside Cars

Many cars today have audio and camera sensors inside of the car, watching and listening to the driver. Audio sensors enable voice commands–for example, “Call Mom”–but to do this they must constantly listen for certain words. In addition, many cars have camera systems that identify if a driver is paying attention. These cameras constantly track the driver’s head position and eye position. For example, GM’s “Super Cruise” system “works with infrared lights to track

[1] Gemini, "Image of exterior and interior camera, radar, and lidar sensor systems on a car," image, generated by Chris Miller, April 21, 2026, Google, https://gemini.google.com

head position and eye gaze," according to GM documentation.[2] Ford's "driver-facing camera checks the driver's eye gaze and head position–even when they are wearing sunglasses," the company reports.[3] Chinese cars have similar capabilities.

Sensors inside cars are potentially highly valuable intelligence collection capabilities–but only under certain conditions. If the data is processed locally and quickly deleted, the risk is low. If not, the risk is substantial.

C. Sensors Mapping the Outside World

Even relatively simple cars today have multiple sensors that track the environment around the car. Cameras, radars, lidars, and ultrasound sensors enable safety systems like automatic braking as well as semiautonomous driving systems, such as advanced cruise control and lane changing.

Cars with more autonomous capabilities tend to have even more sensors. The newest Tesla models use eight cameras for functions from parking assistance to supervised autonomous driving.[4] The Mercedes-Benz Drive Pilot L3 autonomous technology employs thirty sensors, a combination of cameras, radar, LiDAR, ultrasonic sensors, and antennae.[5] Waymo's newest technology uses twenty three sensors of various types, thirteen of which are cameras.[6]

As cars become more autonomous, they'll get more capable at mapping the world around them. We'll have more cameras and lidars gathering data from our streets. Certain types of external sensors create more risks. Ultrasonic sensors with short ranges–used for example in parking-assistance systems–may not offer sufficient fidelity or distance to be of interest to foreign intelligence services. By contrast, cameras and lidars, which provide longer distance and high fidelity pictures, are used by autonomous driving companies to build vast datasets of America's roads. These datasets will unlock new autonomous capabilities. They do so by providing an extraordinarily detailed and regularly updated picture of America's streets.

II. Relevance of Connected Car Data for Foreign Intelligence Services

---

[2] General Motors, *Super Cruise: Getting to Know* (Buick Quick Reference Guide, 2025), https://contentdelivery.ext.gm.com/bypass/gma-content-api/resources/sites/GMA/content/staging/MANUALS/9000/MA9406/en_US/2.0/GTK_2025_Buick_Super_Cruise_87814708_B.pdf

[3] Ford Motor Company, "BlueCruise: Technology Designed for Trust and Driver Collaboration," *From the Road*, February 2, 2026, https://www.fromtheroad.ford.com/us/en/articles/2026/bluecruise--technology-designed-for-trust-driver-collaboration

[4] Tesla, "Replacing Ultrasonic Sensors with Tesla Vision," *Tesla Support*, September 17, 2025, https://www.tesla.com/en_gb/support/transitioning-tesla-vision

[5] Mercedes-Benz, "DRIVE PILOT," *Mercedes-Benz USA*, accessed April 21, 2026, https://www.mbusa.com/en/drive-pilot

[6] "Waymo's 6th-Gen Driver Goes Live with 42% Fewer Sensors," *Automotive World*, February 2026, https://www.automotiveworld.com/news/waymos-6th-gen-driver-goes-live-with-42-fewer-sensors/

Data produced by the sensors examined above creates two categories of risk. First, the car could provide useful information about its driver to foreign intelligence services. Second, the car's external sensors could provide information about other individuals or the environment the car drives through.

A. Intelligence about the Driver

Only a small fraction of America's drivers are priority targets for China's intelligence services, but as artificial intelligence makes it easier to filter data, all foreign intelligence agencies will gather as much data as they can, even before ascertaining whether a specific piece of data is valuable or not. Unexpected patterns can emerge across a broad range of data points, even if each one on its own seems irrelevant or innocuous.

For certain types of drivers–like those who work for the U.S. government, military, or in critical technology sectors–in-car audio and visual data could be far more valuable. The audio sensor could listen to phone calls or conversations. The camera could gather data for authenticating facial recognition. It is often difficult to determine whether automotive companies have sufficient security protocols–in particular, local processing of data, and strict deletion policies–that could mitigate these risks. In the absence of strong evidence to the contrary, we must assume that Chinese technology providers can be compromised by Chinese intelligence services.

B. Intelligence about the Outside World

In contrast to the audio and visual sensors inside of a car–which have more limited need to store or transmit data–the cameras and lidars outside of a car gather data that is intended to be stored and transmitted. This data is needed to enable ever-larger autonomous driving datasets, but it also enhances the risk. Broad access by a foreign intelligence service to near-real time camera data could allow detailed mapping of critical infrastructure. It could enable tracking of traffic into sensitive locations, like military bases or the Pentagon. Recent research by a Norwegian cybersecurity group led by Tor Indstoy has found that a Chinese NIO brand car has exterior cameras that are capable of facial and license plate recognition.[7]

Foreign intelligence services will try to use automotive data to the maximum extent. Media sources report that Israeli intelligence hacked into Iranian traffic cameras to track the movement of Iranian leadership before striking them. This is not an isolated incident: many intelligence agencies are trying to acquire and aggregate camera data in other countries. In Ukraine, Russian forces hacked into surveillance cameras to collect data on Ukraine's Defense Forces.[8] In a 2025 attack, Russian hackers also targeted 10,000 connected cameras at Ukraine's

[7] Tor Indstøy and Arild Tjomsland, "Lion Cage: The Societal Risks of Software Defined Vehicles," (presentation, The Lion Cage Project, Kollektivtrafikk.no, January 2026), https://kollektivtrafikk.no/app/uploads/2026/01/Presentasjon-Lion-Cage.pdf.
[8] Andy Greenberg, "From Ukraine to Iran, Hacking Security Cameras Is Now Part of War's Playbook," *Wired*, March 6, 2026, https://www.wired.com/story/from-ukraine-to-iran-hacking-security-cameras-is-now-part-of-wars-playbook/.

borders to track shipments of Western aid.[9] Ukraine has reportedly employed these techniques against Russia.[10]

If data gathered by cars' cameras and lidars is treated carefully, these risks can be managed. However, we lack sufficient visibility into the cyber security and privacy guarantees around automotive data. Researcher Tor Indstoy has highlighted significant risks associated with a Chinese-manufactured NIO electric vehicle that he purchased in Norway. His team analyzed the flow of data from this car and found that around ninety percent of its data was sent to China.[11] Data packets were continuously transmitted, even when the car appeared to be powered off. Around seventy percent of communications were encrypted, making it hard to audit exactly what information is being sent.[12] The driver's voice commands to the car, this research found, were also transmitted outside the car.[13] The intelligence value of this type of data is significant.

III. Sabotage Risk: Could Foreign Actors Disable Vehicles at Scale?

Espionage isn't the only risk associated with connected cars. If millions of U.S. cars stopped working simultaneously, the economic, political, and potentially even military impact would be substantial. The U.S. government and military's response to a crisis could be impaired if thousands of personnel could not reach their workplaces. Logistics would be imperiled if roads were snarled due to disabled cars. According to media reports, the U.S. intelligence community has previously found extra communications equipment in certain types of critical infrastructure, like port cranes, raising concerns that in a crisis this equipment might be used to disable the equipment.

Could something similar happen with cars? There are two main vectors by which a car might be disabled.

A. Software Systems

---

[9] David Klepper, "Russian Hackers Target Organizations in US and Globally in Cyberattack Aimed at Ukraine Aid, NSA Says," *AP News*, May 22, 20245, https://apnews.com/article/russia-cyberattack-ukraine-aid-nsa-6308ca3e11c8299470df573e4f422878; National Security Agency, Federal Bureau of Investigation, and Cybersecurity and Infrastructure Security Agency, "Russian GRU Cyber Actors Target Global Critical Infrastructure and Logistics," Cybersecurity Advisory, April 2026, https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF.

[10] Greenberg, "From Ukraine to Iran."

[11] Jordan Robertson, "Probing a $69,000 Chinese Electric Vehicle for Clues on Spying," *Bloomberg News*, May 15, 2024, https://www.bloomberg.com/news/newsletters/2024-05-15/probing-a-69-000-chinese-electric-vehicle-for-clues-on-spying.

[12] Tor Indstøy, "Project Lion Cage Part 4: How Much Data and What Kind from a Car to China?" *LinkedIn*, January 2026, https://www.linkedin.com/pulse/project-lion-cage-part-4-how-much-data-what-kind-from-tor-indst%C3%B8y/.

[13] Tor Indstøy, "Part 6: Voice Control Functions—Where and How Are They Processed Within the Car?" *LinkedIn*, August 29, 2023, https://www.linkedin.com/pulse/part-6-voice-control-functions-where-how-processed-within-indst%C3%B8y/

The operation of cars is today defined by their software, so changes to the software can affect how–or whether–cars operate. Today cars receive software updates over the air, just like devices from phones to computers. A malicious software update could potentially disable the operation of a car.

B. Battery Management Systems

Electric vehicles use software to manage their batteries, which is referred to as "battery management systems." If these battery management systems can be changed via over-the-air software updates, it raises the risk that batteries–and thus vehicles–could be disabled. A manipulated battery management system could also cause a battery to set fire.[14]

Norwegian researchers from the public transit authority recently examined whether Chinese manufactured buses operating in Norway faced such a risk. They ran a series of tests, including driving a bus deep into a mine to disable its connectivity features. They found that the Chinese manufacturer of the battery had unlimited ability to update the battery management system in ways that could function as a kill switch.[15]

IV. Visibility into Software and Data Architecture

U.S. government officials have much less visibility than they should into the operation of automotive software and data governance. Indeed, auto companies often appear to have surprisingly limited visibility into their own supply chains and software. Even very detailed studies of automotive cyber security have concluded with substantial uncertainty about how certain types of data is collected or where it is transmitted to.

The auto industry has been impacted by a series of supply chain crises in recent years–over semiconductors and rare earth magnets–that illustrate how some legacy automotive firms in the U.S. (and Europe and Japan) face severe structural difficulties in managing China-related supply chain risk. First, despite repeated warnings about China's ability and willingness to compromise supply of simple semiconductors to the automotive supply chain, car firms nevertheless faced major disruptions when China in 2025 restricted exports of chips from China made by the company Nexperia. Similarly, global auto production was imperiled when China announced export controls on rare earth magnets in early 2025, even though Beijing had spent the previous several years ramping up export controls on critical minerals. In other words, the auto industry has failed to demonstrate that it is capable of managing its own China-related supply chain risk.

[14] Network and Information Systems (NIS) Cooperation Group, *Risk Assessment on Connected and Automated Vehicles* (European Commission and ENISA, January 30 2026), https://www.ccam.eu/wp-content/uploads/2026/03/NIS-Cooperation-Group-Risk-assessment-on-Connected-and-Automated-Vehicles.pdf

[15] Indstøy and Tjomsland, "Lion Cage"

The security of automotive software is difficult to assess, partly because legacy automotive companies use software from many different vendors. Different components in a car often have software written by different companies. U.S. rules now limit the use of certain types of Chinese-origin software in cars, though one car company executive publicly said his company finds it "challenging" to ensure that automotive data is not transmitted to China.[16]

V. China's Regulations on Connected Vehicles and Vehicle Data

China treats connected cars as a national security issue given that they generate large volumes of geospatial, traffic, and other sensor data.[17] Since 2021, the Ministry of Industry and Information Technology has issued rules requiring companies to establish formal systems for classifying data, protecting sensitive information, and managing cybersecurity risks.[18]

These rules mandate that data collection must be minimized where possible. Companies are encouraged to process data within the vehicle itself rather than externally, and "important data" must be stored locally within China.[19] Data considered "important" and thus requiring localization include traffic pattern data, sensitive geographic data, and externally captured video. Any export of this data requires government security review. Recent updates have expanded the definition of "important data" to include information generated not only during vehicle operation but also across R&D and manufacturing.[20]

China also imposes company-specific limitations. In 2021, Beijing restricted the use of Tesla vehicles by Chinese military personnel and employees of government agencies, explicitly citing data security concerns.[21] These restrictions were relaxed after Tesla passed a data security

---

[16] Stephen Wilmot, "The Car Industry Is Racing to Replace Chinese Code," *Wall Street Journal*, February 5, 2026, https://www.wsj.com/business/autos/the-car-industry-is-racing-to-replace-chinese-code-6b939e1f.

[17] Center for Eastern Studies, *Smartphones on Wheels*.

[18] U.S. Commercial Service, "China Data Regulations for Connected Vehicles," *International Trade Administration*, January 6, 2022, https://www.trade.gov/market-intelligence/china-data-regulations-connected-vehicles

[19] Cyberspace Administration of China, *"Several Provisions on the Management of Automobile Data Security (Trial Implementation)"* (August 20, 2021), https://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm

[20] Carolyn Bigg and Amanda Ge, "China: New Guidance on Data Transfer and Identification of Important Data in the Automotive Sector," *Privacy Matters (DLA Piper)*, February 4, 2026, https://privacymatters.dlapiper.com/2026/02/china-new-guidance-on-data-transfer-and-identification-of-important-data-in-the-automotive-sector/

[21] Keith Zhai and Yoko Kubota, "China to Restrict Tesla Use by Military and State Employees," *Wall Street Journal*, March 19, 2021, https://www.wsj.com/world/china/china-to-restrict-tesla-usage-by-military-and-state-personnel-11616155643.

review and agreed to store data locally in China.[22] However, the company has continued to face regular reviews of its software and data protection by the Chinese government.[23]

VI. Other Countries' Policy Responses

A. Norway

Norway has led Europe's reassessment of the security impact of Chinese connected cars. Following a technical audit of Chinese-manufactured Yutong buses in Oslo, Norwegian transport authority Ruter found that the vehicles were equipped with undisclosed, unencrypted SIM cards that routed data through third-party countries like Romania back to servers in China.[24] This created a "kill switch" vulnerability, whereby a foreign manufacturer or state actor could potentially remotely deactivate an entire fleet of buses. To mitigate this risk, the transport authority is implementing firewalls to ensure control and developing stronger cybersecurity requirements for future procurement.[25]

B. Denmark

Danish state-owned transportation company Movia is formally reviewing its cybersecurity risk assessments for its bus fleets following the findings in Norway. Danish authorities say there are no known cases of buses being deactivated, but the company is exploring measures to mitigate vulnerabilities.[26]

C. The European Union

The EU recently introduced a new ICT Supply Chain Security Toolbox and released updated risk assessments for connected and automated vehicles.[27] The EU found substantial data protection risks posed by connected cars, noting:

---

[22] Trefor Moss, "Tesla to Store China Data Locally in New Data Center," *Wall Street Journal*, May 26, 2021, https://www.wsj.com/business/autos/tesla-to-store-china-data-locally-in-new-data-center-11622015001.

[23] Reuters, "Tesla halts driving-assistance software trial in China, pending approval," March 24, 2025, https://www.reuters.com/business/autos-transportation/tesla-says-will-release-fsd-feature-china-after-software-approval-2025-03-24/.

[24] Stephen Wilmot and Ed Ballard, "Can Chinese-Made Buses Be Hacked? Norway Drove One Down a Mine to Find Out," *Wall Street Journal*, November 19, 2025, https://www.wsj.com/business/can-chinese-made-buses-be-hacked-norway-drove-one-down-a-mine-to-find-out-fbda755f.

[25] Associated Press, "Norway Transport Firm Steps Up Controls After Tests Show Chinese-Made Buses Can Be Halted Remotely," *AP News*, November 5, 2025, https://apnews.com/article/ruter-yutong-china-norway-electric-buses-931f3dbdab3f82402da68cbcb31f856b.

[26] Ibid.

[27] European Commission, "EU Launches New Toolbox to Strengthen ICT Supply Chain Security," *Press Release MEX/26/411*, February 12, 2026, https://ec.europa.eu/commission/presscorner/detail/en/mex_26_411.

"a series of top risks pertaining to high-risk suppliers subjected to, e.g., government or military pressure to implement hidden and malicious hard- or software, updates or configurations in their products or changing the functioning of in-vehicle automated driving systems. A supplier can leverage both known and hidden direct access pathways to the vehicle as an attack vector…Moreover, such attackers can leverage normal over-the-air updates, another top risk scenario identified to prevent immediate detection. [The automotive cybersecurity regime]...was mainly created to ensure traffic safety and does not sufficiently mitigate against such risks."

However, the EU has not mandated steps to address these risks, both because Europe is divided over China policy and because key European automakers are deeply entangled with China.

D. Britain

The British government has moved to formalize cybersecurity standards through the 2024 Automated Vehicles (AV) Act, which allows the deployment of self-driving vehicles while letting the government revoke licenses if cybersecurity standards are not met.[28] It mandates "security by design," or that that security must be built into the vehicle from the outset through its entire lifecycle. The Connected & Automated Mobility (CAM) 2025 strategy commits the government to develop a legislative framework rather than relying on voluntary industry standards.[29] Further, the UK Ministry of Defence reportedly banned EVs containing Chinese components from certain military sites.[30]

E. Poland

The Polish Ministry of National Defence recently banned Chinese-made vehicles from entering protected military areas, reflecting concerns about data collection.[31] State-backed Polish think tank OSW has recently published high quality analysis on the risks of Chinese-origin connected vehicles.

F. Israel

[28] UK Parliament, "Automated Vehicles Act 2024," *Public General Acts*, May 20, 2024, https://www.legislation.gov.uk/ukpga/2024/10/contents.
[29] Great Britain, Department for Transport, Connected and Automated Mobility 2025: Realising the Benefits of Self-Driving Vehicles in the UK (London: Department for Transport, August 2022), https://assets.publishing.service.gov.uk/media/62ff438c8fa8f504cdec92df/cam-2025-realising-benefits-self-driving-vehicles.pdf
[30] Richard Holmes, "Electric Cars with Chinese Parts Banned from Military Sites over Spying Fears," *iNews*, April 2025, https://inews.co.uk/news/electric-cars-chinese-parts-banned-from-military-sites-spying-fears-3644639
[31] Reuters, "Poland bars Chinese-made cars from military sites over data security fears," February 18, 2026, https://www.reuters.com/business/aerospace-defense/poland-bars-chinese-made-cars-military-sites-over-data-security-fears-2026-02-18/.

According to reports, Israeli authorities have banned Chinese-manufactured vehicles from military bases. They have also encouraged or required senior military officials not to use Chinese vehicles.[32]

VII. U.S. Policy Response

The United States has taken several important steps to limit vulnerabilities in the automotive space, though more remains to be done.

A. The ICTS Connected Vehicle Rule

The U.S. Commerce Department has limited deployment of software and certain types of communications equipment sourced from adversary governments via the "Connected Vehicle Rule," which took force in 2025. This rule aims to ensure that the most critical autonomy and data-transfer equipment on a car are not designed or manufactured in China.

However, the ICTS office in the Commerce Department has been inactive during the Trump administration–despite that the first Trump administration created the office and the authorities on which it rests. Congress should bolster the U.S. government's ability to regulate Chinese technology by providing a stronger legislative basis for the ICTS office and by mandating reports into the risks posed by Chinese auto components and software, as well as in related sectors like datacenters, industrial equipment, internet of things modules, and robotics.

B. Battery Management Systems

The Commerce Department's "Connected Car" rule addresses many concerns about vehicle operating software being impacted by malicious Chinese software updates. However, Chinese battery firms have signaled that they want to invest in the U.S., and American auto firms are reportedly exploring joint ventures with Chinese firms. If U.S. firms consider the use of Chinese batteries in American electric vehicles, it is critical that regulations strictly prohibit use of Chinese-origin battery management systems.

C. Data Regulation

In 2024, the U.S. government issued an executive order (EO 14117) banning transfer to China and other adversaries of bulk data with personally identifiable information. If this executive order is being fully complied with, some of the intelligence collection risks outlined above would be mitigated. However, data collection and transfer practices in the auto industry are currently highly opaque, making it difficult to ascertain which type of automotive data is considered to be limited by the executive order. The U.S. government should mandate additional disclosures about data protection and transfer in the auto industry. It should also support and make public more research about cyber security practices in the auto sector.

[32] Center for Eastern Studies, *Smartphones on Wheels*.

D. Allied Engagement

Most other countries lack robust regulations to protect themselves from Chinese espionage and potential sabotage operations in their auto fleet. European countries already operate large and growing numbers of Chinese cars. Canadian Prime Minister Mark Carney has recently announced plans to reduce tariffs on Chinese EVs, which will lead to more Chinese cars in Canada. Across Southeast Asia, Chinese cars are now widespread. It is highly plausible that, in a military crisis in the Taiwan Strait, China could use the threat of sabotage to pressure third countries. Europe is particularly vulnerable to this type of coercion. The U.S. government should engage with other countries on this topic to mitigate risks of Chinese espionage and coercion.

Conclusion

Protecting the cybersecurity of connected and increasingly autonomous cars is not only critical for the safety of our transportation systems. Cars are a major source of sensor data and thus of great interest to foreign intelligence services. Recently imposed limits via the ICTS authority on use of critical components and software from China are an important step in protecting the U.S. from espionage and sabotage in this sector. Yet as U.S. auto firms reportedly seek joint ventures with Chinese manufacturers, these limitations must be protected and expanded. In addition, more testing and disclosure is needed to ensure that auto companies and firms in the auto supply chain are fully complying with restrictions on data transfer to China.

Autos are also a test case. All types of physical AI and robotics systems–from smarter industrial equipment, to drones, to humanoids–raise similar risks of surveillance and sabotage if their critical systems are not protected. Striking the right balance in the auto industry will provide a template for other sectors—ensuring either that we're well protected, or that we're increasingly vulnerable, as the number of sensors proliferates and the volume of data gathered grows.