

LASER FOCUS: COUNTERING CHINA'S LIDAR THREAT TO U.S. CRITICAL INFRASTRUCTURE AND MILITARY SYSTEMS

BY CRAIG SINGLETON AND RADM (RET.) MARK MONTGOMERY

DECEMBER 2, 2024

INTRODUCTION

“Only by mastering crucial core technologies within our own hands,” said Chinese Communist Party General Secretary Xi Jinping, “can we [China] truly seize the initiative in competition and development, and fundamentally safeguard our national economic security, national security, and security in other domains.”¹ Xi’s declaration underscores his desire to transform China into a science and technology great power, which, he argues, hinges on tightening “international production chains’ dependence on China.”² LiDAR, a remote sensing technology with both military and civilian applications, stands at the center of Beijing’s bid for technological superiority.

Xi’s technological vision is not just an ambition — it is already materializing. Today, Chinese companies are rapidly consolidating control over the global LiDAR market, with PRC-origin sensors now widely deployed across civilian and military networks worldwide, including in the United States. These sensors often serve as essential nodes within interconnected public safety, transportation, and utility systems, which is a clear benefit to the United States. However, Chinese LiDAR’s system-wide integration also leaves its users vulnerable to espionage and sabotage, potentially enabling Beijing to access sensitive U.S. data or disrupt critical operations.

For decades, Beijing has used cyber operations to breach sensitive networks and infiltrate critical infrastructure in the US.³ China’s military and intelligence services could leverage Chinese-made LiDAR systems for espionage

1. “Core technology depends on one’s own efforts: President Xi,” *People’s Daily* (China), April 19, 2018. (<https://web.archive.org/web/20240601110352/http://en.people.cn/n3/2018/0419/c90000-9451186.html>)

2. “China Focus: Xi Calls for Developing China Into World Science and Technology Leader,” *Xinhua* (China), May 29, 2018. (https://web.archive.org/web/20240427223530/http://www.xinhuanet.com/english/2018-05/29/c_137213175.htm); Ben Murphy, “Xi Jinping: Certain Major Issues for Our National Medium- to Long-Term Economic and Social Development Strategy,” *Center for Security and Emerging Technology*, November 10, 2020. (https://web.archive.org/web/20240914165234/https://cset.georgetown.edu/wp-content/uploads/t0235_Qiushi_Xi_economy_EN-1.pdf)

3. “People’s Republic of China Cyber Threat,” *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, accessed October 3, 2024. (<https://web.archive.org/web/20241003131848/https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,” February 7, 2024. (<https://web.archive.org/web/20241008172548/https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>); U.S.-China Economic and Security Review Commission, “Section 2: China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States,” 2022. (https://web.archive.org/web/20240928011205/https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf)

purposes, much as they have exploited the compromised communication gear sold by Chinese telecommunications giant Huawei.⁴ The widespread adoption of Chinese-made LiDAR technology also advances Xi’s “comprehensive national security” (总体国家安全) concept, which merges technological development with state security to enhance China’s geopolitical advantage.⁵ In practice, Beijing could weaponize Western reliance on Chinese-made systems by manipulating or disrupting LiDAR supply chains as it has done repeatedly with rare earth elements to pressure other countries into accepting its strategic demands.

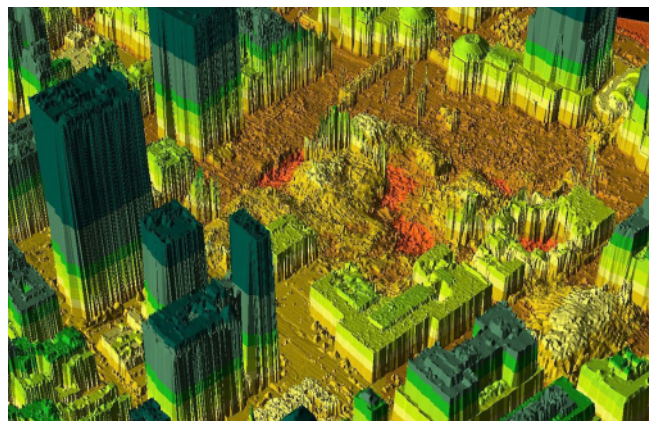
This memo provides an overview of LiDAR technology, detailing its expanding use across the United States. Next, it examines how LiDAR operates and how China could exploit the broad adoption of PRC-made LiDAR sensors to facilitate espionage or sabotage of critical U.S. networks and infrastructure. Finally, the memo outlines actionable steps policymakers can take to prevent Chinese exploitation of LiDAR technologies and protect U.S. national security.

Countering Chinese LiDAR dominance requires integrating LiDAR into a comprehensive industrial policy that bolsters U.S. technological leadership and economic competitiveness. This approach must go beyond simply reducing reliance on untrusted vendors from foreign countries of concern. It should also focus on expanding domestic LiDAR production capacity and fostering trusted supply-chain partnerships with allied nations. Establishing and enforcing rigorous cybersecurity standards for LiDAR technology will also be essential to safeguarding critical infrastructure and ensuring LiDAR’s secure integration into both civilian and military networks.

LIDAR BACKGROUNDER

LiDAR (or Light Detection and Ranging) is an advanced remote sensing technology that uses laser pulses to create highly detailed, three-dimensional maps of surrounding environments. By calculating the time it takes for these pulses to return to a sensor, LiDAR can generate precise spatial data far exceeding traditional methods, like radar and sonar. While LiDAR was originally developed in 1961 by Hughes Research Laboratory for lunar exploration, it has evolved into an indispensable tool in a wide range of civilian and military applications worldwide.⁶

The technology’s most well-known civilian application is in the autonomous vehicle (AV) industry, where LiDAR sensors enable real-time object detection and safe navigation



LiDAR image of World Trade Center collapse site shows area topography; darker red marks lower elevations. (Photo by NYC Office of Emergency Management/Getty Images)

4. Katie Bo Lillis, “FBI Investigation Determined Chinese-Made Huawei Equipment Could Disrupt US Nuclear Arsenal Communications,” CNN, July 25, 2022. (<https://web.archive.org/web/20241008064218/https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html>); U.S. Federal Communications Commission, “Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation,” June 30, 2020. (<https://web.archive.org/web/20240830010448/https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf>); Eva Dou, “Documents Link Huawei to China’s Surveillance Programs,” *The Washington Post*, December 14, 2021. (<https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/>)

5. Katja Drinhausen and Helena Legarda, “‘Comprehensive National Security’ Unleashed: How Xi’s Approach Shapes China’s Policies at Home and Abroad,” *Mercator Institute for China Studies*, September 15, 2022. (<https://web.archive.org/web/20240918020038/https://www.merics.org/en/report/comprehensive-national-security-unleashed-how-xis-approach-shapes-chinas-policies-home-and>)

6. Juan Carlos Fernandez Diaz, William E. Carter, Ramesh L. Shrestha, and Craig L. Glennie, “Lidar Remote Sensing,” *Springer Reference*, 2017, pages 757-808. (https://web.archive.org/web/20180611222950/https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-7671-0_44)

in dynamic driving environments. LiDAR has also been integrated into drone, train, and airport transportation systems for similar purposes. Additionally, utility companies and critical infrastructure providers are increasingly using LiDAR to monitor pipelines, power lines, and rail networks, proactively identifying structural weaknesses and environmental hazards before they compromise system integrity.

Urban planners are also integrating LiDAR with artificial intelligence and machine learning to build so-called “safe cities.”⁷ For example, many cities rely on LiDAR sensors to monitor traffic flows at major road intersections and automatically adjust traffic signals to reduce congestion. LiDAR-enabled alerts can also provide emergency responders with critical, real-time information about vehicle accidents and other safety hazards, enabling more efficient response times. Lastly, LiDAR can optimize city services, such as waste management and energy distribution, by delivering precise data on usage patterns and infrastructure conditions, streamlining resource allocation, and enhancing public safety.⁸

LiDAR’s applications are becoming essential to modern military and defense systems, too. U.S. reconnaissance and missile guidance systems rely on LiDAR to enhance target acquisition, terrain analysis, and navigation in hostile environments. Looking toward the future of warfare, the Department of Defense’s Joint All-Domain Command and Control initiative aims to integrate data and technology across military platforms to improve battlefield awareness, which will include outfitting next-generation autonomous military vehicles and drones with fully integrated LiDAR suites.⁹ For instance, the U.S. Army’s Future Vertical Lift program, focused on developing advanced helicopters, will rely on LiDAR for real-time terrain mapping and obstacle avoidance capabilities.¹⁰

Military Applications of LiDAR

- **Battlefield Mapping:** Enables precise terrain analysis, including in urban environments.
- **Enemy Detection:** Helps locate enemy positions and infrastructure.
- **Navigation:** Enhances movement by providing detailed spatial awareness.
- **Sea Mine Detection:** Identifies the depth of underwater threats.
- **Laser Weapon Support:** Predicts performance by analyzing atmospheric conditions.
- **High-Altitude Surveillance:** Systems like DARPA’s HALOE map large areas rapidly from the air, offering advanced data collection over 100,000 feet above ground.

7. Tom Grey, “How Lidar Powers Smart Cities and Protects Privacy,” *Ouster*, May 1, 2020. (<https://web.archive.org/web/20240523092021/https://ouster.com/insights/blog/how-lidar-powers-smart-cities-and-protects-privacy>); Ana Rouxinol, “Why Smart Cities Use LiDAR Sensors?” *Aerial Precision Blog*, January 27, 2023. (<https://web.archive.org/web/20240414041241/https://www.aerial-precision.com/blog/why-smart-cities-use-lidar-sensors>); Jon Barad, “How Lidar Can Protect Privacy and Advance Safety in Smart City Applications,” *StateTech*, November 2, 2021. (<https://web.archive.org/web/20240518155114/https://statetechmagazine.com/article/2021/11/how-lidar-can-protect-privacy-and-advance-safety-smart-city-applications>)

8. “Efficient Waste Management with Lidar Technology,” *Recycling Magazine*, October 24, 2023. (<https://web.archive.org/web/20240421015528/https://www.recycling-magazine.com/2023/10/24/efficient-waste-management-with-lidar-technology>)

9. John R. Hoehn, “Joint All-Domain Command and Control,” *Congressional Research Service*, January 21, 2022. (<https://web.archive.org/web/20241007142905/https://sgp.fas.org/crs/natsec/IF11493.pdf>); “How to Ensure Readiness of Next-Generation Defense Technology: Solving the Issue of Massive Heat,” *Breaking Defense*, April 22, 2024. (<https://web.archive.org/web/20240521225526/https://breakingdefense.com/2024/04/how-to-ensure-readiness-of-next-generation-defense-technology-solving-the-issue-of-massive-heat>)

10. Ryan Schradin, “New Vertical Lift Aircraft Creates New Helmet Requirements for Pilots,” *The Modern Battlespace*, November 8, 2023. (<https://web.archive.org/web/20240616181629/https://modernbattlespace.com/2023/11/08/new-vertical-lift-aircraft-creates-new-helmet-requirements-for-pilots>); Sydney J. Freedberg, Jr., “The Army’s Future Vertical Lift Decision,” *Defense.info*, April 2, 2020. (<https://web.archive.org/web/20240614213133/https://defense.info/defense-decisions/2020/04/the-armys-future-vertical-lift-decision>)

China has also prioritized LiDAR as part of its ongoing military modernization. Under its “intelligentized warfare” concept, the People’s Liberation Army (PLA) is integrating LiDAR into defense systems to boost battlefield awareness and precision-strike capabilities.¹¹ LiDAR has reportedly been installed on autonomous Chinese military platforms, including an autonomous fighting vehicle developed by the PLA in partnership with UISEE Technology and Dongfeng Motors. Equipped with advanced LiDAR from Chinese manufacturers such as Hesai, these and other LiDAR-enabled platforms are poised to become a “trump card,” or decisive advantage, in enhancing Chinese reconnaissance operations, according to Chinese state media.¹²



Source: China Central Television broadcast of Hesai LiDAR (circled) on PLA Autonomous Fighting Vehicle (2022)¹³

Today’s use cases aside, LiDAR’s potential remains largely unrealized. The global LiDAR market is projected to exceed \$2.8 billion by 2025, driven by demand for high-resolution mapping, autonomous systems, and automation technologies.¹⁴ North America accounted for 36.6 percent of LiDAR-related revenue in 2021, the highest percentage in the world.¹⁵ While non-Chinese companies in the United States, Germany, Canada, and Israel are key competitors operating on a level playing field, Chinese LiDAR firms benefit from extensive state support, giving them an outsized advantage.¹⁶ This state backing allows Chinese companies to dominate the market, especially in

11. U.S. Department of Defense, “Military and Security Developments Involving the People’s Republic of China 2023,” October 19, 2023. (<https://web.archive.org/web/20241010014818/https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>); “Yanwu Xu, Senior Hardware Design Engineer at Hesai Technology,” *The Org*, accessed October 28, 2024. (<https://web.archive.org/web/20240715125230/https://theorg.com/org/hesai-technology/org-chart/yanwu-xu>); For an explanation of how the East China Research Institute of Electronic Engineering/ECRIEE is an alias of the CETC 38th Research Institute and their defense technology development activities, see, for example: Wendell Minnick, “China Reveals Origin of AEWC Radar,” *DefenseNews*, March 14, 2016. (<https://www.defensenews.com/pentagon/2016/03/14/china-reveals-origin-of-aewc-radar>)

12. James Mulvenon, “Hesai Technology (禾赛科技) and its “Chinese Eye,” *Dr. James C. Mulvenon*, June 24, 2024. (<https://web.archive.org/web/20240714151237/https://w5499a.p3cdn1.secureserver.net/wp-content/uploads/2024/06/Hesai-Technology-Final.pdf>)

13. Ibid.

14. “LiDAR Market Worth \$2.8 Billion by 2025,” *Markets Insider*, June 30, 2020. (<https://markets.businessinsider.com/news/stocks/lidar-market-worth-2-8-billion-by-2025-exclusive-report-by-marketsandmarkets-1029354541>); Pierrick Boulay and Yu Yang, “What – or Who – is a Safe Bet in ADAS in 2024? – Automotive 2023 review, Part II,” *Yole Group*, December 14, 2023. (<https://www.yolegroup.com/strategy-insights/what-or-who-is-a-safe-bet-in-adas-in-2024-automotive-2023-review-part-ii>)

15. “LiDAR Market Size & Trends,” *Grand View Research*, accessed October 28, 2024. (<https://web.archive.org/web/20240806103410/https://www.grandviewresearch.com/industry-analysis/lidar-light-detection-and-ranging-market>)

16. Karen M. Sutter and Kelley M. Saylor, “U.S.-China Competition in Emerging Technologies: LiDAR,” *Congressional Research Service*, May 15, 2024. (<https://web.archive.org/web/20240904015220/https://crsreports.congress.gov/product/pdf/IF/IF12473>); U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, “Gallagher, Krishnamoorthi Applaud Inclusion of New Chinese Companies, including Hesai Technology, On DoD’s Chinese Military Companies List,” February 2, 2024. (<https://web.archive.org/web/20240927201505/https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-krishnamoorthi-applaud-inclusion-new-chinese-companies-including>)

price-sensitive sectors, with Chinese firms accounting for more than 80 percent of global LiDAR sales.¹⁷ As LiDAR adoption grows, China's market dominance could provide Beijing with strategic leverage across other emerging industries, such as precision agriculture, renewable energy, and advanced robotics.

LIDAR FUNCTIONALITY AND KNOWN RISKS

LiDAR's transformative potential is undeniable, but its rapid proliferation carries significant risks. The technology's ability to collect and transmit precise spatial data makes it a prime tool for espionage and sabotage, especially when these systems are manufactured or otherwise controlled by companies located in foreign countries of concern. These risks are set to intensify as LiDAR systems are increasingly deployed near critical infrastructure, transportation hubs, utility grids, and defense nodes across the United States.

China has long recognized LiDAR's strategic value. In 2018, China identified LiDAR as a critical "chokepoint technology," and in 2020, Beijing directed that LiDAR be integrated into military systems.¹⁸ Through its military-civil fusion strategy, which mandates that Chinese companies collaborate with China's defense and intelligence agencies, Beijing has blurred the lines between civilian and military technologies.¹⁹

At least one Chinese LiDAR company, Hesai, has acknowledged in investment disclosures that the Chinese government "may influence or intervene" in its "operations at any time."²⁰ Such disclosures highlight the inherent national security risks associated with embedding PRC-manufactured LiDAR systems in U.S. and foreign infrastructure.²¹ While Hesai denies any affiliation with China's military, its inclusion on the Defense Department's Section 1260H list, which designates companies linked to the Chinese military-industrial complex, underscores the U.S. government's concerns. Notably, after Hesai's legal challenge briefly led to its removal from the 1260H list in October 2024, the Defense Department promptly re-listed the company "based on the latest information."²²

Chinese law not only facilitates military-civil fusion, it mandates cooperation between Chinese companies and state security agencies. China's 2017 National Intelligence Law, 2021 Data Security Law, and recently revised Counter-Espionage Law require Chinese companies, including LiDAR manufacturers, to assist state intelligence

17. Dhruva Gogoi, "BriefCASE: Chinese Suppliers Gain Strong Foothold in Global Lidar Market," *S&P Global*, June 26, 2024. (<https://www.spglobal.com/mobility/en/research-analysis/briefcase-chinese-suppliers-gain-strong-foothold-lidar-market.html#:~:text=Specialist%20suppliers%20from%20mainland%20China,on%20a%20strong%20growth%20trajectory>)

18. Xi used the term 卡脖子, translated as "chokepoint," although the term literally means "to strangle" or "to have someone in a stranglehold." Ben Murphy, "Xi Jinping: Speech at the Symposium of Scientists," *Center for Security and Emerging Technology*, September 11, 2020. (<https://web.archive.org/web/20240721122927/https://cset.georgetown.edu/publication/xi-jinping-speech-at-the-symposium-of-scientists>); "智能汽车创新发展战略 [Smart Car Innovation and Development Strategy]," *China National Development and Reform Commission*, February 2020. (<https://perma.cc/4BCC-UNLV>)

19. Emily de La Bruyère and Nathan Picarsic, "Defusing Military-Civil Fusion: The Need to Identify and Respond to Chinese Military Companies," *Foundation for Defense of Democracies*, May 2021, page 7. (<https://web.archive.org/web/20240827204137/https://www.fdd.org/wp-content/uploads/2021/05/fdd-monograph-defusing-military-civil-fusion.pdf>)

20. U.S. Securities and Exchange Commission, Corporate Filing, Registration Number 333-269247, "Hesai Group," February 2, 2023. (https://web.archive.org/web/20240904015423/https://www.sec.gov/Archives/edgar/data/1861737/000110465923009861/tm2120356-22_fla.htm)

21. U.S. Department of Justice, Office of Public Affairs, Press Release, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," January 31, 2024. (<https://web.archive.org/web/20241007101741/https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>)

22. David Shepardson, "Hesai returned to US list of firms alleged to help Beijing's military," *Reuters*, October 16, 2024. (<https://www.reuters.com/technology/pentagon-removes-lidar-maker-hesai-us-list-firms-alleged-help-beijings-military-2024-10-16>)

operations.²³ China's National Intelligence Law, for example, explicitly requires "all organizations and citizens" to support, assist, and cooperate with national intelligence efforts.²⁴ This legal framework extends far beyond China's borders, potentially enabling the Chinese government to exploit PRC-manufactured LiDAR systems abroad. This jeopardizes the security of any nation that integrates Chinese-made LiDAR into its networks and critical infrastructure systems.

China's exploitation of civilian technologies for espionage and sabotage purposes is well documented. As FBI Director Christopher Wray testified in 2024, "China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike."²⁵ The U.S. Department of Commerce has also warned that adversaries could exploit networked devices, including surveillance cameras, drones, and other connected systems, such as LiDAR.²⁶ Similarly, the Department of Defense recognizes that China is actively targeting U.S. critical infrastructure, aiming to disrupt societal functions and interfere with military operations during both peace and wartime.²⁷

Despite these and other known risks, the methods that adversaries such as China could use to exploit LiDAR technology remain poorly understood. Understanding exactly how LiDAR works and how foreign adversaries could exploit its known vulnerabilities is key to preventing its misuse.

HOW LiDAR WORKS AND ADVERSARIAL RISKS

LiDAR sensors are equipped with high-speed optical transceivers, including laser emitters and photodetectors, which enable them to transmit and receive information through light pulses. Modern LiDAR systems use coded light pulses, or "fingerprints," to distinguish their signals from background noise and reduce interference from other sensors.²⁸ With each new generation of LiDAR, the sophistication of pulse encoding increases, potentially introducing more serious risks.

Specifically, as pulse codes become more complex, adversaries could develop new methods to manipulate these signal patterns, potentially using them to interfere with LiDAR systems and the broader networks to which they are connected. This could involve designing "fingerprints" that disrupt LiDAR sensor functionality, including the disabling of a sensor's safety features.

23. "Data Security Law of the PRC," *China Law Translate*, June 10, 2021. (<https://web.archive.org/web/20241008224553/https://www.chinalawtranslate.com/en/datasecuritylaw>); "Counter-Espionage Law of the P.R.C. (2023 ed.)," *China Law Translate*, April 26, 2023. (<https://web.archive.org/web/20240927000745/https://www.chinalawtranslate.com/en/counter-espionage-law-2023>)

24. "PRC National Intelligence Law (as Amended in 2018)," *China Law Translate*, June 27, 2017. (<https://web.archive.org/web/20240926192544/https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017>)

25. Christopher Wray, "Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party," *Testimony before the House Select Committee on Strategic Competition between the United States and the Chinese Communist Party*, January 31, 2024. (<https://web.archive.org/web/20241007040526/https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party>)

26. Securing the Information and Communications Technology and Services Supply Chain, U.S. Department of Commerce, 15 Federal Register 4909, January 19, 2021. (<https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain>)

27. U.S. Department of Defense, Press Release, "DOD Support to National Security Memorandum 22," May 7, 2024. (<https://www.defense.gov/News/Releases/Release/Article/3766979>)

28. "Pandar128," *Hesai*, accessed October 28, 2024. (<https://web.archive.org/web/20240917172128/https://www.hesaitech.com/product/pandar128>)

As LiDAR's signal processing capabilities advance, each sensor's supporting hardware is also becoming more sophisticated, further increasing the risk of exploitation. This vulnerability arises from several factors. First, LiDAR sensors utilize advanced embedded processors and non-volatile memory to store firmware, operational logs, and other information. The complexity of these advanced processors could allow for the introduction — and concealment — of malicious code or firmware backdoors that are difficult to detect and neutralize, even upon close inspection.

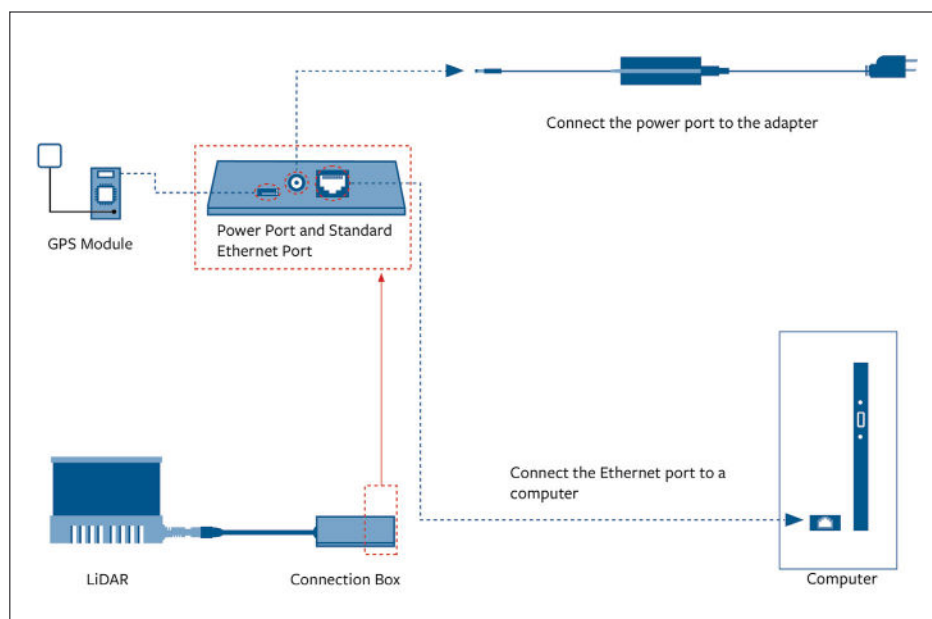


Figure 1: Standard LiDAR connection box (power, ethernet, GPS).

The incorporation of advanced custom silicon chips in many newer LiDAR sensors, especially those produced in China, presents another layer of risk. These custom chips can be specifically engineered to include hidden vulnerabilities, known as “hardware trojans,” which could provide a LiDAR company or other hostile actor with unauthorized access or control over LiDAR devices.

Furthermore, LiDAR sensors often rely on embedded operating systems, such as Linux, and use Ethernet standards for data transmission. As a result, these sensor systems typically connect to the broader internet, significantly increasing their vulnerability to cyberattack. For instance, many LiDAR sensors include a built-in web interface, accessible via a standard browser and powered by an onboard web server. These web interfaces, if not properly secured, could be remotely accessed and manipulated by hackers or LiDAR companies located in foreign countries of concern to gain control over deployed LiDAR sensors and potentially LiDAR-enabled networks.

What is more, LiDAR systems frequently receive software updates over the internet, often affecting network settings, cybersecurity protocols, and core sensing algorithms. These over-the-internet updates, especially those originating in foreign countries of concern, could introduce additional cybersecurity vulnerabilities, making Chinese-made LiDAR systems highly vulnerable to manipulation.²⁹

Given these hardware and software configurations, LiDAR systems produced by companies located in foreign countries of concern, or otherwise beholden to adversarial governments, are highly vulnerable to two specific cybersecurity threats: disruptive attacks that could disable or misdirect the technology, and unauthorized data exfiltration that could compromise sensitive information.

29. S M Mostaq Hossain, Shampa Banik, Trapa Banik, and Ashfak Md Shibli, “Survey on Security Attacks in Connected and Autonomous Vehicular Systems,” *arXiv*, October 14, 2023. (<https://web.archive.org/web/20231017015253/https://arxiv.org/abs/2310.09510>)

DISRUPTIVE CYBERATTACKS

Like other connected technologies, LiDAR systems are inherently vulnerable to cyberattacks. However, these risks increase significantly when sensors are manufactured in, or by companies beholden to, foreign countries of concern. Foreign adversaries or the companies they control could potentially embed malicious code in the encrypted components found in most LiDAR sensors, making detection extremely difficult. These types of compromises raise serious cybersecurity risks, particularly because LiDAR's integration into supply chains and transportation networks creates single points of failure. Manipulating even a small number of sensors could have widespread repercussions.

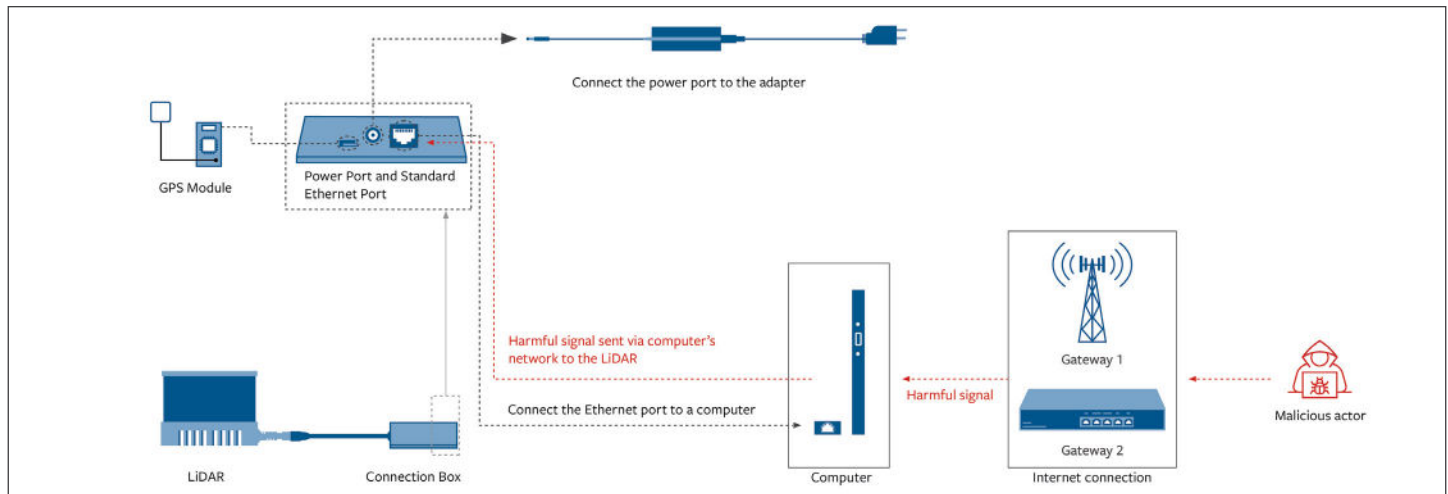


Figure 2: Illustrative example of a network attack.

LiDAR sensors, as networked devices often connected via Ethernet and linked to systems with internet access, are highly vulnerable to a specific type of disruptive cyberattack known as a network-based attack.³⁰ These attacks commonly rely on malware, which can be embedded at multiple stages: during manufacturing, network integration, or through routine firmware updates. Once malware is installed, attackers can remotely access LiDAR sensors via internet-connected pathways (or access points), potentially disabling the sensors or manipulating them to malfunction or transmit false information.

For example, after gaining remote access to one of these compromised networks, cyber actors could instruct LiDAR sensors to send false fingerprints to other nearby sensors, causing them to malfunction. Such an attack could result in targeted disruptions or the disabling of select safety systems in these networks. In extreme cases, it could cause widespread failures of entire LiDAR-dependent systems, leading to large-scale disruptions in public safety and national defense operations, such as paralyzing autonomous vehicle networks or hindering critical infrastructure monitoring.

The threat of attacks that cause LiDAR sensors to transmit false information is equally severe. Compromised sensor activity could erode policymaker confidence in the reliability of LiDAR-dependent systems, including advanced weapons platforms. This potential loss of faith could undermine strategic decision-making and policymaker resolve to deploy these systems during future conflicts. During wartime, LiDAR-enabled weapons could fail when

30. Ibid.

needed most. Similarly, sensor malfunctions could sow doubt about the integrity of LiDAR-dependent critical infrastructure systems. This extends to systems needed to support future force mobilization, such as domestic rail networks, potentially jeopardizing U.S. military readiness and responsiveness.

Another type of disruptive cyberattack targeting LiDAR systems is an optical attack, in which an adversary sends coded light pulses directly to the sensor's lens. Unlike network-based attacks, optical attacks do not require internet connectivity, making them difficult to detect. The only known mitigation for optical attacks is to use LiDAR sensors from a trusted source, though even this relies on the assumption that the sensors have not been tampered with during manufacturing or distribution.

This vulnerability becomes clear when considering how an optical attack could be executed. Modern LiDAR sensors transmit and receive “fingerprints” over long distances, even at very low signal levels. These fingerprints reduce interference by ensuring each LiDAR system can identify its unique signal. However, a malicious manufacturer under the control of an adversarial nation could embed malware that activates upon detecting a second, hostile “fingerprint.” In such a scenario, an external light source could transmit this adversarial fingerprint to compromised LiDAR sensors, triggering adverse effects as soon as the hostile signal is recognized.

An adversarial fingerprint could disable the sensor immediately or trigger it to stop functioning at a pre-determined point in the future. In many respects, these optical attacks resemble electronic warfare techniques such as GPS jamming. Unlike jamming, however, they do not require continuous interference. A single instance of interference could potentially disable thousands of LiDAR sensors, leading to widespread disruption across the systems that depend on them, such as those that monitor critical infrastructure.³¹

The malware necessary to carry out an optical attack could be embedded in the LiDAR sensor during its manufacturing process or introduced later via routine firmware updates. For instance, malicious code could be hidden deep within the millions of transistors found in the custom silicon chips used in modern LiDAR receivers, making it nearly impossible to detect prior to or after deployment.

Moreover, given the extreme sensitivity of modern LiDAR receivers, these types of optical attacks could be delivered from ground-based and airborne systems. For example, an attack could be initiated by something as simple as an individual using a handheld laser device to send the adversarial “fingerprint” to nearby LiDAR sensors. To cover larger geographic areas, delivery would likely involve high-altitude balloons and/or aircraft equipped with ground-directed laser systems.

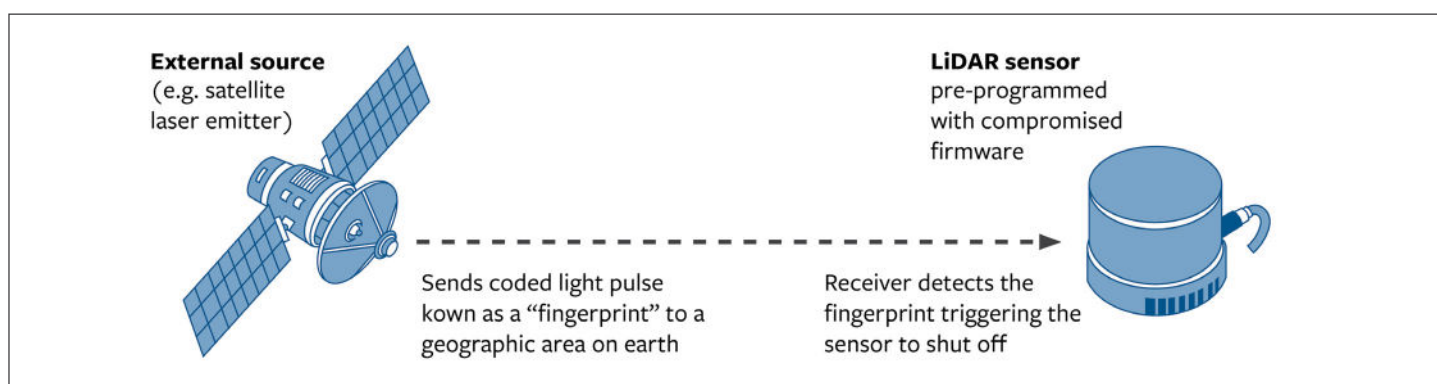


Figure 3: Illustrative example of an optical attack.

31. Ibid.

Importantly, the emitted signal does not need to strike the LiDAR sensor directly to achieve its intended effect, as LiDAR systems are designed to detect faint secondary reflections from distant objects. This means that even if the sensor is shielded from direct exposure, an optical attack could succeed by illuminating the general area within several hundred meters of a LiDAR sensor.

Satellite-based laser systems, similar to those already deployed on remote monitoring satellites, could also disable compromised LiDAR sensors in critical areas across the United States within seconds. For instance, a satellite emitting a laser beam with a 5-meter diameter at Earth's surface and a pulse repetition frequency of 10 megahertz could deliver an optical attack across a 60-square-kilometer area, the size of Manhattan, in just 0.3 seconds. An area the size of Washington, DC, (160 square kilometers) could be targeted in approximately 0.8 seconds.

China's advancements in satellite-based laser systems, such as those observed in recent orbital missions, heighten the risk of Beijing using space-based technologies to disable compromised LiDAR sensors. Last year, a Chinese satellite, the Daqi-1, was observed using its onboard laser system to take measurements around the Hawaiian Islands.³² Additionally, Chinese state media reported that a Chinese Changguang remote sensing satellite successfully demonstrated space-to-ground laser links.³³ These examples indicate that Chinese-controlled satellite laser systems are already in orbit with the demonstrated capability to conduct optical attacks across wide geographic regions, including within the United States.

UNAUTHORIZED DATA EXFILTRATION

While disruptive cyberattacks can occur through network-based and optical methods, data exfiltration usually requires an internet connection to covertly transmit sensitive information abroad. This is an area where China has long excelled. In 2018, Chinese hackers breached U.S. Navy defense contractors, stealing data related to undersea warfare and missile programs.³⁴ Similarly, in 2021, Huawei was found to have transmitted sensitive data from surveillance systems installed at the African Union headquarters to servers in China for over five years.³⁵

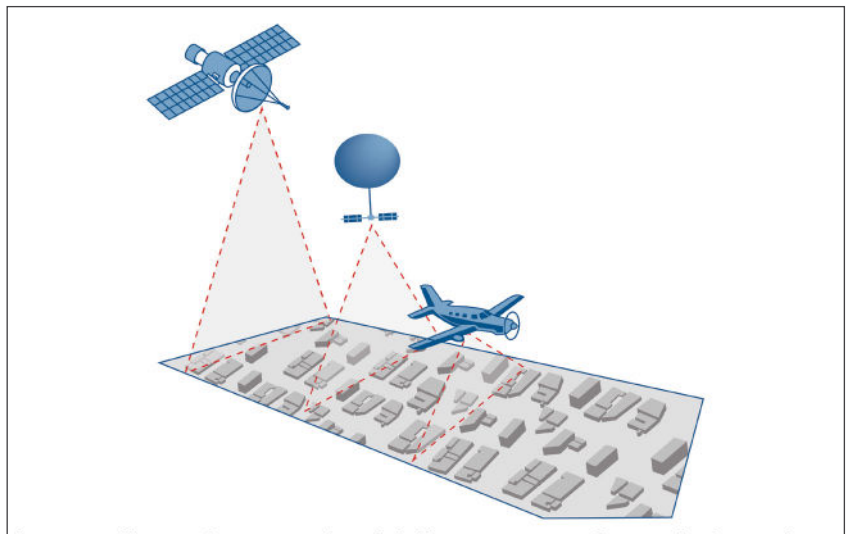


Figure 4: Illustrative example of delivery systems for optical attacks.

32. Bryce Moore, "Chinese Satellite Beams Green Lasers Over Hawaii," *The Hill*, February 13, 2023. (<https://web.archive.org/web/20240709003819/https://thehill.com/policy/technology/3854939-chinese-satellite-beams-green-lasers-over-hawaii>)

33. Jia Liu, "Company Makes Satellite Communication Breakthrough," *Chinese Academy of Sciences*, June 30, 2023. (<https://perma.cc/L65V-5HP2>)

34. Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *The Washington Post*, June 8, 2018. (https://web.archive.org/web/20240627090029/https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html)

35. Ghalia Kadiri and Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," *Le Monde* (France), January 27, 2018. (https://web.archive.org/web/20241009101748/https://lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html)

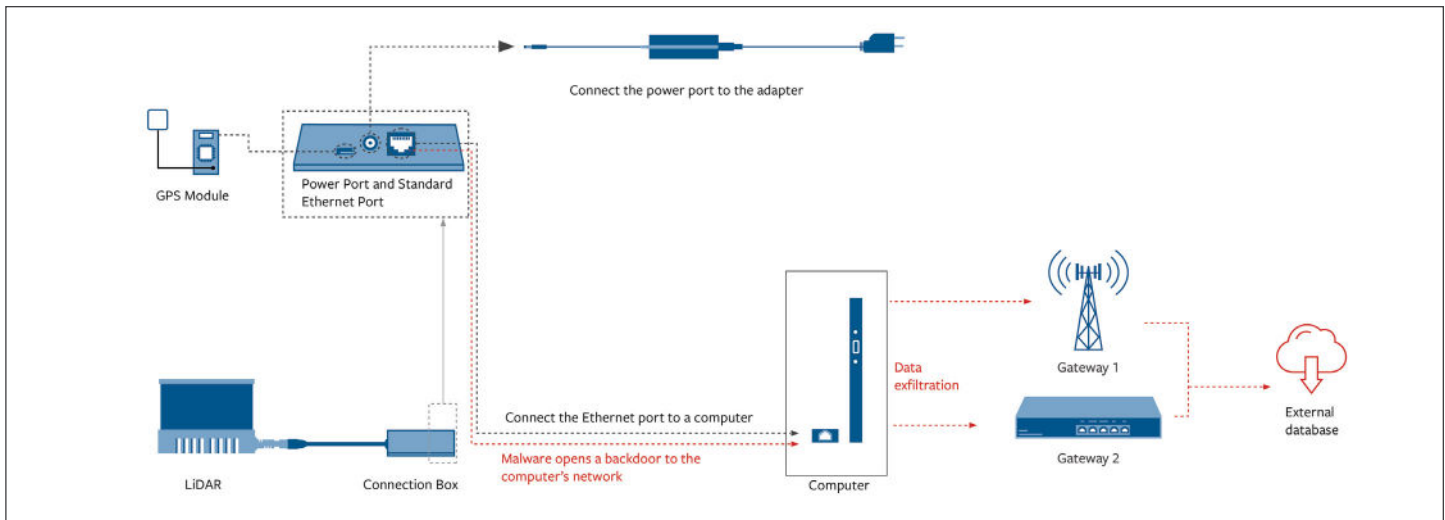


Figure 5: Illustrative example of data exfiltration.

These and other documented examples show how China leverages unauthorized data exfiltration to conduct both military and industrial espionage.

Recent intelligence warnings underscore the serious threat posed by LiDAR systems linked to foreign countries of concern, particularly with regard to unauthorized data exfiltration in the automotive sector. An Estonian Foreign Intelligence Service bulletin revealed that a Chinese LiDAR manufacturer planned to transmit data collected from vehicles in Estonia back to China.³⁶ The unnamed Chinese company was reportedly developing LiDAR systems for self-driving cars in Estonia that would scan the local environment and transmit this information to Beijing. Although data collected for autonomous driving is typically deleted if non-essential, this Chinese firm intended to transfer all environmental data to a China-based database, raising concerns about the potential exploitation of this technology for Chinese intelligence purposes, such as mapping foreign infrastructure, identifying sensitive locations, or tracking patterns of movement.

Other industries using LiDAR face similar vulnerabilities. The absence of standardized cybersecurity regulations across sectors leaves safeguarding efforts decentralized, with protection varying widely by industry. This sector-by-sector approach results in weak and inconsistent security measures, with many users lacking the knowledge or protocols to prevent data from being covertly transmitted to adversarial entities.

An additional data exploitation risk stems from the fact that an increasing number of LiDAR manufacturers, including those from China, are offering cloud-backed software with their sensor systems. These solutions are often sold to state and local governments in the United States for applications such as traffic management. However, much of the data collected by these systems is stored by the manufacturer.³⁷ If the manufacturer is located in China, it is legally obligated

36. Estonian Foreign Intelligence Service, “The Advance of Chinese Technology,” February 2024. (<https://raport.valisluureamet.ee/2024/en/6-china/6-3-the-advance-of-chinese-technology>)

37. “OmniVidi Perception Service Software Platform,” *Seyond*, accessed October 28, 2024. (<https://web.archive.org/web/20240927114709/https://www.seyond.com/products/omnividi-preview>); “DJI FlightHub 2,” *DJI Enterprise*, accessed October 28, 2024. (<https://web.archive.org/web/20241007113032/https://enterprise.dji.com/flighthub-2>); “Q-Track,” *Quanergy*, accessed October 28, 2024. (<https://web.archive.org/web/20240910045449/https://quanergy.com/products/q-track>); “HyperVision 1.0,” *RoboSense*, accessed October 28, 2024. (<https://web.archive.org/web/20240827111429/https://www.robosense.ai/en/rslidar/HyperVision1>); “Gemini,” *Ouster*, accessed October 28, 2024. (<https://web.archive.org/web/20241008233311/https://ouster.com/products/software/gemini>)

to share information with the Chinese government, including military and intelligence agencies. This creates a direct pathway for Beijing to access and exploit sensitive U.S. data, including the ability to analyze traffic patterns, infrastructure layouts, and other critical data that could inform military, cyber, or espionage operations targeting U.S. cities.

One notable example of such exploitation was the recent “Cloud Hopper” cyber-espionage campaign, attributed to a hacker group linked to China’s Ministry of State Security.³⁸ The campaign targeted foreign cloud service providers, exploiting vulnerabilities to steal intellectual property and sensitive government data from companies and organizations across several industries.³⁹ This incident highlights how Chinese cyber actors can leverage cloud services, potentially including those tied to LiDAR manufacturers, to access vast amounts of sensitive information.⁴⁰

LIMITATIONS OF CURRENT CYBERSECURITY PROTOCOLS AND CERTIFICATIONS

A LiDAR manufacturer under the influence of a foreign country of concern could embed malware in devices in ways that are nearly impossible for customers or third-party cybersecurity organizations to detect. While cybersecurity standards such as ISO/SAE 21434 and ISO/IEC 27001 provide best practices for automotive cybersecurity and information security management, they are not designed to safeguard products sourced from untrustworthy manufacturers.

Most cybersecurity certifications are essentially compliance checks that rely on information provided directly by the manufacturer and rarely include a review of source code. Auditors typically examine documentation about the manufacturer’s development processes and cybersecurity protocols and then certify products based on whether this documentation meets established standards. These certifications presume the manufacturer is trustworthy and the information provided is accurate.

However, certifications alone cannot guarantee the security of a particular product. A LiDAR manufacturer located in or otherwise beholden to a foreign country of concern could easily program hidden malware into its devices that would evade typical detection techniques by cybersecurity auditors. Detecting the malware would require significant penetration testing, which is expensive, highly technical, and uncommon.

A recent event illustrates the limitations of existing cybersecurity protocols and certifications in detecting firmware errors or malware in Chinese LiDAR sensors. On March 1, 2024, at precisely 12:00 a.m. Coordinated Universal Time (UTC), two LiDAR sensor models produced by Chinese manufacturer Hesai were involved in a global, synchronized disruption. This disruption was caused by a firmware error that failed to account for 2024 being a leap year.⁴¹ The sensors incorrectly calculated timestamps after being synchronized to UTC, which is the standard used by LiDAR systems. The result was the grounding of autonomous vehicle fleets in both China and the United States due to timing mismatches between Hesai’s LiDAR sensors and the vehicles themselves.⁴²

38. Jack Stubbs, Joseph Menn, and Christopher Bing, “Inside the West’s failed fight against China’s ‘Cloud Hopper’ hackers,” *Reuters*, June 26, 2019. (<https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper>)

39. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, “Awareness Briefing: Chinese Cyber Activity Targeting Managed Service Providers,” February 2019. (<https://web.archive.org/web/20230718085502/https://www.cisa.gov/sites/default/files/c3vp/Chinese-Cyber-Activity-Targeting-Managed-Service-Providers.pdf>)

40. Price Waterhouse Cooper, “Operation Cloud Hopper,” April 2017. (<https://web.archive.org/web/20240917182317/https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf>)

41. “Hesai Technology Addresses Lidar Products Bug,” *Pandaily*, February 29, 2024. (<https://web.archive.org/web/20240301031704/https://pandaily.com/hesai-technology-addresses-lidar-products-bug>)

42. Ibid.

The affected LiDAR models, the Hesai Pandar 40 and QT, are commonly used in U.S. autonomous vehicles. Several hundred vehicles were impacted during this incident, with some fleets grounded for over 24 hours. Zoox, a U.S. autonomous vehicle company, was the first to alert Hesai to the issue. While this incident was almost certainly the result of an unintended firmware error, not malware, it went unnoticed by Hesai's customers and by third-party cybersecurity organizations that had certified Hesai's products — until the malfunction shut down vehicle fleets.

This event underscores how a malicious attack using an intentional time trigger could cause far more widespread disruption if significant numbers of compromised LiDAR systems from adversarial nations were deployed in consumer vehicles or critical infrastructure. If an unintentional error like this can go undetected by cybersecurity auditors and customers, intentionally hidden malware would likely prove equally elusive.

POLICY RECOMMENDATIONS

LiDAR sensors are becoming crucial for automating and controlling key U.S. infrastructure, including dockyards, drawbridges, traffic signals, and autonomous vehicles. As LiDAR deployment accelerates — particularly in connected vehicles — millions of these systems will be operating across the United States in the coming years. LiDAR's rapid expansion heightens security risks, particularly when sensors are sourced from countries of concern, such as China. These vulnerabilities could severely compromise U.S. infrastructure and defense systems.



Figure 6: Illustrative example of potential impacts of disruptive cyberattacks.

The U.S. government is beginning to address the security risks posed by Chinese technology. In late September 2024, the Department of Commerce's Bureau of Industry and Security proposed a rule to ban the sale or importation of connected vehicles using specific Vehicle Connectivity Systems (VCS) and Automated Driving Systems (ADS) linked to China or Russia.⁴³ This includes telematics, cellular, and satellite modules in VCS and ADS software. However, this proposed rule does not explicitly cover LiDAR systems or other use cases beyond vehicles, leaving many broader vulnerabilities unaddressed.

43. U.S. Department of Commerce, Bureau of Industry and Security, Press Release, "Commerce Announces Proposed Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats," September 23, 2024. (<https://web.archive.org/web/20241007223623/https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign>)

To address the risks posed by adversary-influenced LiDAR systems, U.S. policymakers must prioritize LiDAR in America's broader industrial policy. This includes fostering domestic LiDAR competition and building strong public-private partnerships between American LiDAR manufacturers, the U.S. government, and key civilian stakeholders, such as utility and car companies. These and other proactive measures will be necessary to avoid costly "rip-and-replace" scenarios in the future, akin to ongoing efforts to remove untrusted Huawei telecommunications gear from U.S. networks.

Other potential steps to address critical LiDAR-related vulnerabilities and safeguard U.S. infrastructure include the following:

STRENGTHENING ICTS SCRUTINY OF LiDAR UNDER COMMERCE DEPARTMENT AUTHORITIES

- **Expand ICTS Review to Include LiDAR Systems:** The Commerce Department's Information and Communications Technology and Services (ICTS) unit should explicitly include LiDAR systems as a category for future national security reviews.
- **ICTS Unit Risk Assessments and Mandatory Disclosures for LiDAR Providers:** The ICTS unit at the U.S. Department of Commerce should mandate that companies importing LiDAR systems from countries of concern provide detailed disclosures about the hardware, software, and security features of their products. Security vulnerabilities should be publicly disclosed, particularly those that could affect critical infrastructure. The next U.S. administration should consider issuing an executive order to enhance these requirements, utilizing the ICTS unit's existing regulatory authorities to ensure thorough risk assessments for high-risk technologies, including LiDAR, from countries of concern.
- **Ban the Use of PRC-Made LiDAR in Critical Sectors:** ICTS, under its existing authorities from Executive Order 13873, should evaluate the risks posed by Chinese-manufactured LiDAR in critical infrastructure sectors such as transportation, energy grids, public safety, and defense systems. If deemed necessary, ICTS should consider restricting the procurement of Chinese-made LiDAR in these sectors, much like it has done with Huawei and ZTE equipment.

BLOCKING CHINESE LiDAR FROM DoD SUPPLY CHAINS:

- **Maintain Hesai on the Chinese Military Companies List:** Congress and the Department of Defense should ensure that Chinese LiDAR manufacturers, including Hesai and others potentially connected to the Chinese military, are thoroughly investigated and remain listed on the Defense Department's Chinese Military Companies list. This designation restricts their access to U.S. markets and prevents their integration into American defense systems, safeguarding national security.
- **Legislate a Ban on DoD Procurement of Chinese LiDAR Sensors:** Congress should consider including legislation in the National Defense Authorization Act to explicitly ban the Department of Defense from procuring LiDAR sensors manufactured by companies based in foreign countries of concern. This ban could mirror other recent legislation prohibiting the department from procuring problematic Chinese-made battery systems.

ENHANCING CYBERSECURITY STANDARDS FOR LiDAR SYSTEMS

- **Establish Sector-Specific Cybersecurity Standards for LiDAR:** The National Institute of Standards and Technology (NIST), along with the Cybersecurity and Infrastructure Security Agency (CISA), should develop sector-specific cybersecurity standards for LiDAR systems in critical infrastructure, such as traffic management and smart cities. Congress should consider passing legislation requiring NIST to establish these standards and mandating compliance by federal contractors and grant recipients.
- **Mandate Regular Penetration Testing and Audits of LiDAR Systems:** Public- and private-sector LiDAR users should be required to conduct regular penetration testing and cybersecurity audits to ensure their systems are resilient against unauthorized access or manipulation. Congress could consider amending the Federal Information Security Modernization Act to include specific provisions for connected systems, including LiDAR.

REGULATING LiDAR DATA USAGE AND PREVENTING DATA EXFILTRATION

- **Enforce Strict LiDAR Data Localization Requirements:** All data collected by U.S. government entities and state/local governments using LiDAR systems should be stored domestically to prevent data exfiltration. Congress could consider amending the CLOUD Act or the International Emergency Economic Powers Act to mandate data localization requirements for LiDAR technology.
- **Develop a National Framework for LiDAR Data Security in Transportation Networks:** The Department of Transportation (DoT), in coordination with the Transportation Security Administration at the Department of Homeland Security (DHS), should create a national framework for securing LiDAR data in autonomous vehicles and traffic management systems. This framework should mandate encryption standards, data retention policies, and data-sharing restrictions.

U.S. STATE-LEVEL ACTION ON PROCUREMENT AND REGULATION

- **Enact State-Level Procurement Bans for Chinese LiDAR Systems:** State legislatures should consider adopting procurement bans on PRC-made LiDAR technologies for public infrastructure systems, similar to how states such as Texas and Florida have enacted targeted bans on Chinese drones.

BUILDING TRUSTED LiDAR SUPPLY CHAINS WITH ALLIED AND PARTNER NATIONS

- **Launch a “Trusted LiDAR” Supply Chain Initiative:** The United States should partner with allies such as Germany, Canada, South Korea, Israel, and Japan to build secure LiDAR supply chains, ensuring these systems meet high cybersecurity standards for use in civilian and military sectors. Congress could also consider legislation to provide targeted tax incentives and subsidies for domestic or allied LiDAR production. This would be similar to the incentives offered to semiconductor producers under the CHIPS Act, albeit on a much smaller scale.
- **Develop a NATO Working Group on Emerging LiDAR Risks:** The United States should initiate a NATO (North Atlantic Treaty Organization)-led assessment of LiDAR’s cybersecurity risks in joint military operations. This effort would include developing countermeasures against potential cyber and optical attacks on LiDAR. The Department of Defense should propose establishing a permanent NATO working group dedicated to these concerns, with support from member states’ military cybersecurity units.

EMPOWERING LAW ENFORCEMENT AND REGULATORY AGENCIES

- **Evaluate the Feasibility of DoT Procurement Bans:** Congress could consider legislation that would ban the DoT from procuring LiDAR sensors manufactured by companies based in foreign countries of concern. Such measures could also restrict the use of DoT funds, such as SMART Grants, to ensure they are not used for acquiring LiDAR systems produced by these entities.
- **Increase and Enforce Section 301 Tariffs on Chinese LiDAR:** The U.S. Trade Representative should consider increasing the existing 25 percent tariff on LiDAR imports from China to 50 percent or higher to counter unfair competition caused by state subsidies and oversupply practices in China. Additionally, Customs and Border Protection should be tasked with investigating past LiDAR imports from Chinese companies to ensure proper enforcement of tariffs. This would help protect U.S. LiDAR manufacturers from predatory pricing and support a more competitive domestic market.
- **Create a DHS Task Force on Emerging LiDAR Threats:** DHS, through CISA, should create an inter-agency task force focused on emerging threats posed by LiDAR systems, with a particular emphasis on vulnerabilities in transportation and critical infrastructure. The task force should release regular public reports on vulnerabilities, mitigation strategies, and incident response planning for cyberattacks targeting LiDAR systems.
- **Expand the ‘Covered List’ to Include Chinese LiDAR Manufacturers:** The Federal Communications Commission (FCC) should add Chinese LiDAR manufacturers to its “Covered List” of banned entities, preventing U.S. companies from using federal subsidies to purchase these systems. Congress could also direct the FCC to investigate this issue through new legislation, if needed.
- **Conduct an ODNI-Led Technical Threat Assessments for Foreign LiDAR Systems:** The Office of the Director of National Intelligence (ODNI) should lead inter-agency efforts to conduct comprehensive technical threat assessments on LiDAR systems sourced from foreign adversaries. These assessments would evaluate cybersecurity vulnerabilities, espionage risks, and supply-chain concerns, providing crucial intelligence for protecting U.S. infrastructure and military capabilities.

INCREASING PUBLIC AWARENESS AND TRANSPARENCY

- **Require Transparency for Municipal LiDAR Deployments:** Municipal governments deploying LiDAR systems in public infrastructure projects (such as smart cities) should be required to notify the federal government about the source of the technology and whether it originates from a foreign country of concern. This transparency measure will allow communities to make informed decisions about the technology being integrated into their environment. Congress should require such disclosures as part of federal grant conditions, mandating that recipients of federal infrastructure funding disclose technology sources.

CONCLUSION

China’s rapid advancements in LiDAR technology, underpinned by state-led initiatives and Xi’s comprehensive national security strategy, present escalating risks to critical infrastructure, defense systems, and technological independence. As Beijing seeks to expand its influence over LiDAR supply chains, the United States and its allies must implement robust policies to secure their own LiDAR capabilities and protect against foreign exploitation. Acting now to address these vulnerabilities will safeguard national security and preserve the resilience of vital technological ecosystems.

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's China Program

Leveraging the full scope of economic, financial, military, political, cyber, and technology tools, FDD's China Program exposes and challenges the wide-ranging threats posed by the Chinese Communist Party. FDD's China team includes experts with Chinese-language skills, data-driven mining capabilities to examine Chinese language sources, and experience in government, intelligence, the military, and the technology sector.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment.

Craig Singleton is a senior fellow at FDD, where he also serves as senior director of FDD's China Program. He previously spent more than a decade as a senior U.S. diplomat, completing multiple overseas assignments in the Middle East, Latin America, and East Asia. While stationed in Washington, DC, Craig focused on developing policies aimed at confronting China's malign influence activities and North Korea's nuclear weapons program.

RADM (Ret.) Mark Montgomery is the senior director of the Center on Cyber and Technology Innovation at FDD. He also directs CSC 2.0, having served as the Cyberspace Solarium Commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.