FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

China's Internet-of-Everything Gambit and Battle for LiDAR

By Emily de La Bruyère and Nathan Picarsic

June 28, 2024

Introduction

The Chinese government is intent on seizing control of emerging technologies to cement a dominant position in tomorrow's economic and security environment.[1] A principal focus of Beijing's efforts is the network of physical devices known as the Internet of Things (IoT), which Chinese sources expect to become an "Internet-of-Everything" once it achieves a "global scale."[2] In the realm of hardware, Beijing faces little competition. Chinese IoT module makers already dominate the global market in areas ranging from smart appliances to autonomous cars, including a full stranglehold over the commercial drone industry.[3] Government support and industrial strategy, as well as technology pilfered from abroad, have fueled this advantage.[4]

Light detection and ranging (LiDAR) technology is a clear example of this People's Republic of China (PRC) strategy, which Beijing employed previously in its conquest of the drone market. China's dominance there has made it difficult for the Pentagon to contribute to drone warfare operations in places like Ukraine without relying on Chinese inputs. LiDAR, like drone technology, is dual-use relevant and key to emergent critical infrastructure.[5] Today, Chinese entities are dominating the commercialization of LiDAR and its applications in current advanced driver assistance systems and autonomous driving, a critical emerging field.

The United States, its allies, and the private sector must respond to the risk of China's LiDAR gambit with both defensive and offensive measures. It will be necessary to protect U.S. research and development efforts while publicizing the risk of partnerships with Chinese Internet-of-Everything players. An effective response in the LiDAR field can serve as a model for related efforts since similar threats proliferate across the Internet of Everything.

1. Emily de La Bruyère and Nathan Picarsic, "There's a Bigger Threat Than Big Tech. It's Big China," *Defense One*, July 26, 2020. (https://www.defenseone.com/ideas/2020/07/theres-bigger-threat-big-tech-its-big-china/167187/?oref=defenseone_today_nl)
2. Li Xiaotong, 订物互联 [*Internet of Everything*] (Beijing: People's Posts and Telecommunications Press, 2017).
3. For a recent market share assessment, see: Ed Alvarado, "Ranking the Leading Drone Manufacturers," *Drone Industry Insights*, November 28, 2023. (https://droneii.com/ranking-the-leading-drone-manufacturers). Alvarado notes that "the first place by a substantial margin goes to DJI."
4. Lynn Walford, "The Who, What, When, Where, Why, and How of Lidar," *Auto Futures*, February 11, 2019. (https://www.autofutures.tv/topics/the-who--what--when--where--why--and-how-of-lidar/s/49fb4a79-1a8f-4960-9656-9190847851fb)
5. 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)

Understanding LiDAR

LiDAR is a sensor pod that measures distance with lasers and can deliver high-fidelity, three-dimensional views of surroundings whether in stationary (e.g., near critical infrastructure) or mobile deployments (e.g., robotaxis). Autonomous applications, like driverless cars and the economic and technological boons they promise, demand inputs like LiDAR. Perhaps more importantly, they demand comprehensive approaches to leveraging LiDAR alongside complementary software and hardware advances. This means that an advantage in LiDAR can translate into a commercial advantage.

LiDAR can aid in the characterization of surroundings, including distance and proximity.[6] The technology can be used in a variety of use cases that range from weather sensing to infrastructure safety monitoring. The technology is already a critical input for the majority of the leading autonomous driving players.

LiDAR stands to drastically improve the standard features of currently deployed advanced driver assistance systems (ADAS). Its ability to map the distances of three-dimensional environs at high fidelity and in real time promises to enable more competent and safe autonomous driving — and at scale.

LiDAR is not a silver bullet in autonomous technology. It must be deployed in concert with a broader suite of sensors, including radar and cameras. That suite also requires additional elements that include integrated circuits; resources for storing, fusing, and processing information flows and algorithms; as well as other inputs and outputs. The race to deploy autonomous driving is a race to assemble that complex suite.

While LiDAR might not be the whole answer, car companies that lack the hardware and engineering expertise for LiDAR are likely to be at a disadvantage. Indeed, if Chinese companies capture the LiDAR market and shape its technological development, they will gain a systemic advantage in the autonomous driving competition. BYD, the Chinese electric car company,[7] will have a leg up over global peers if BYD's engineers have preferential access to supply, technical support, and research and development opportunities supported by China's non-market (government) efforts. The Chinese Communist Party's (CCP's) "State-led, Enterprise-driven" economic model has delivered real-world advantages, including in the solar supply chain, where polysilicon dominance has enabled Chinese players to capture the higher-margin module and panel markets.[8]

LiDAR technology also plays a vital role in monitoring critical infrastructure — ranging from transit nodes like bridges and tunnels to power facilities like transformers and power lines[9] — and other industrial autonomy applications. Those critical infrastructure sites include U.S. military installations, which leverage LiDAR alongside other perimeter security and imagery collection technologies to monitor everything from facility conditions to force protection and flight safety missions.[10]

6. Karen Sutter and Kelley Sayler, "U.S.-China Competition in Emerging Technologies: LiDAR," *Congressional Research Service*, August 14, 2023. (https://crsreports.congress.gov/product/pdf/IF/IF12473)

7. BYD may be little known in the U.S. market, but it is one of China's primary auto champions with dominant product offerings in batteries as well as cars; see: Peter Hoskins & Natalie Sherman, "China's BYD overtakes Tesla's electric car sales in last quarter of 2023," *BBC News* (UK), January 2, 2024. (https://www.bbc.com/news/business-67860232)

8. Seaver Wang and Juzel Lloyd, "Reforging the Solar Photovoltaic Supply Chain," *Breakthrough Institute*, February 16, 2023. (https://thebreakthrough.org/issues/energy/reforging-the-solar-photovoltaic-supply-chain)

9. "How LiDAR Works for Infrastructure Inspection in Bridges, Tunnels, Dams, Power Lines," *Neuvition*, September 20, 2023. (https://cdn.neuvition.com/media/blog/infrastructure-inspection.html)

10. Roger Clarke and David Foster, "LiDAR part of digital foundation for installations of future," *Air Force Civil Engineer Center Planning and Integration Directorate*, September 9, 2020. (https://www.af.mil/News/Article-Display/Article/2341922/lidar-part-of-digital-foundation-for-installations-of-future)

Military-Civil Fusion

The Internet-of-Everything promises returns that span from direct revenue flows, access to new pools of capital, and innovation that may fuel next-generation products. This is reflected in the corporate strategies of many of Beijing's "Big Tech" companies. These companies assume that as device connectivity is expanded to a broader array of "smart" real-world objects, they will be in a prime position to control the operating systems that bring the "Internet of Everything" to life.[11] This promises rewards akin to the dominant positions of Microsoft and Google in earlier information technology epochs.[12]

The rise of a new connected future also offers tremendous boons for the Chinese security and strategic apparatus. China's national strategy of military-civil fusion (MCF) is premised on the notion that civilian resources, technologies, and positioning can be leveraged to modernize the People's Liberation Army and the CCP's projection of power.[13]

LiDAR fits neatly within this mandate. Chinese press sources celebrate LiDAR as a "core technology."[14] Autonomy applications in China draw on LiDAR for drone and vehicle use. Chinese media also tout, "applications of lidar in the military field include battlefield reconnaissance, atmospheric environment detection, tracking and fire control, underwater detection, and comprehensive auxiliary applications."[15]

The technology — and its deployment abroad — also enables the surveillance and even disruption of critical infrastructures. For example, LiDAR positioned to monitor the health of a bridge may also capture information about vessels transiting on or around them. LiDAR could pose a risk of remote disruption, which could present operational harm in critical infrastructures and systems. Drones relying on LiDAR, for example, could have their operational performance in swarming compromised by remote disruption. The operational risks with LiDAR may be contested, but a series of security vulnerabilities involving both internal and external threats and difficult-to-defend attack surfaces have been demonstrated.[16] In this way, Chinese LiDAR deployment presents risks similar to those of Chinese juggernauts Huawei and DJI.

Finally, there is the dependence question. Amidst heightened great power competition, U.S. critical and security systems simply cannot depend on Chinese components.[17]

11. "万物互联时代，中国企业实现弯道超车引领全球智能新生态产业链 [In the era of Internet of Everything, Chinese companies have achieved overtaking in corners and led the global smart new ecological industry chain]," Sohu, November 3, 2023. (https://www.sohu.com/a/733484342_120961457)

12. Emily de La Bruyère and Nathan Picarsic, "Worldwide Web: Why China is Taking over the Internet of Things," *The Octavian Report*, Spring 2019.

13. Emily de La Bruyère, "The New Metrics for Building Geopolitical Power in a New World," *The National Interest*, April 12, 2020. (https://nationalinterest.org/feature/new-metrics-building-geopolitical-power-new-world-143147?page=0%2C1)

14. "突破技术封锁，我国强势拿下激光雷达技术，各国得知后纷纷赞叹 [Breaking through the technological blockade, our country has powerfully acquired lidar technology. Countries around the world praised it after learning about it]," *Baijiahao*, January 30, 2019. (https://baijiahao.baidu.com/s?id=1624081385868467853&wfr=spider&for=pc)

15. "2023年中国激光雷达行业应用市场现状分析：应用场景广泛 市场需求将加速释放 [Analysis of the current situation of the application market of China's lidar industry in 2023: Market demand in a wide range of application scenarios will be accelerated]," *Sohu*, June 21, 2023. (https://mil.sohu.com/a/688140463_114835)

16. Robert Hallyburton, Qingzhao Zhang, Z. Morley Mao, and Miroslav Pajic, "Partial-Information, Longitudinal Cyber Attacks on LiDAR in Autonomous Vehicles," March 6, 2023. (https://arxiv.org/abs/2303.03470); Sally Cole Johnson, "LiDAR sensors have fixable security vulnerability," *Laser Focus World*, December 7, 2022. (https://www.laserfocusworld.com/test-measurement/article/14286616/lidar-sensors-have-fixable-security-vulnerability)

17. For a recent demonstration of the attendant risks, see: Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, "Cybersecurity Guidance: Chinese-Manufactured UAS," January 17, 2024. (https://www.cisa.gov/resources-tools/resources/cybersecurity-guidance-chinese-manufactured-uas); Craig Singleton, "Securing Communications Networks from Foreign Adversaries," *Testimony before the House Committee on Energy and Commerce*, February 15, 2024. (https://www.fdd.org/analysis/2024/02/15/securing-communications-networks-from-foreign-adversaries)

Strategic Responses

Individual Chinese LiDAR companies are part of a broader Chinese industrial policy agenda. LiDAR itself is just one technology within a broader Chinese Internet-of-Everything ambition. A strategic response is needed. The U.S. government needs to play both defense and offense to compete.

The defensive effort should begin with protecting U.S. research and development. As with commercial drones, LiDAR is a story of U.S.-origin technology being harvested by China's tech machine and scaled with non-market support. Trade protections and intellectual property theft recourse are necessary to defend against such measures. The United States Trade Representative (USTR) should launch a Section 301 investigation of China's non-market trade practices across the Internet-of-Everything ecosystem. Ultimately, tariffs should be considered for components (like compound semiconductors used in LiDAR) to finished LiDAR, camera, and related products. In concert, U.S. capital and technology should be prohibited from supporting the Chinese Internet-of-Everything players in Beijing's surveillance program, including those complicit in the genocide of the Uyghur ethnic minority. Those restrictions should be executed across entire sectors, rather than dealing in entity-specific bans.

But those are just first steps: The power of the U.S. market should be leveraged to support American and allied solutions. This should include prohibiting the acquisition of Chinese-made technologies that present security risks and provide support to military- and surveillance-tied actors. Similarly, the Department of Commerce's Entity List designations should include every Chinese LiDAR company. The U.S. government should also consider designations of Chinese military-linked actors managed by the Departments of Treasury and Defense.[18] Such actions would broadcast the risks of PRC players and dependence on them in both interagency and private sector fora. Addressing Chinese industrial policy as codified in the National Defense Authorization Act's Section 1260H, the United States can better address the wider threat.

However, an effective strategy needs more than U.S. government restrictions. The U.S. capital market needs to recognize the fiduciary risks associated with Chinese Internet-of-Everything players. These companies carry human rights and security concerns that fly in the face of Environmental, Social, and Governance investment standards. Indeed, these PRC companies' operations are vulnerable to U.S. regulatory risk. However, they are also subject to the Chinese Communist Party's "techlash" and restrictions on "important data" and the far reach of the PRC's data localization and National Intelligence legal regimes.[19] Those are the factors that prompted the abrupt de-listing of Chinese ride-hailing giant Didi from the New York Stock Exchange in 2022, causing U.S. investors to lose billions of dollars. The same factors could at any point impact the status of Chinese LiDAR companies traded on U.S. exchanges. Any corporate boards, underwriters, or exchanges that overlook this risk in bringing new IPOs to the market are willingly exposing themselves to shareholder litigation and competitive risks.

18. For outputs from the 2021 National Defense Authorization Act's Section 1260H, see: Department of Defense, News Release, "DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," October 5, 2022. (https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/#:~:text=Section%201260H%20directs%20the%20Department,with%20additional%20entities%20as%20appropriate)

19. Elaine Dezenski and Joshua Birenbaum, "Congress just touching the TikTok tip of the iceberg of China's spying," *New York Post*, April 10, 2024. (https://nypost.com/2024/04/10/opinion/congress-just-touching-the-tiktok-tip-of-the-iceberg-of-chinas-spying); Emily de La Bruyère and Nathan Picarsic, "A 'techlash' with Chinese characteristics," *TechCrunch*, November 21, 2021. (https://techcrunch.com/2021/11/21/a-techlash-with-chinese-characteristics)

Working with Chinese companies could also negatively impact U.S. supply chains dependent on those companies. U.S. players — whether in autos or critical infrastructure — must address their own procurement processes to pursue trusted solutions over Chinese offerings. Otherwise, China's vision for an Internet-of-Everything world operating according to Chinese rules will be one step closer to reality. Should that happen, U.S. security and international norms will suffer. U.S. supply chains and commercial advantage will suffer, too, and likely first.

If a strategic approach to competing — and protecting American markets and values — is pursued by regulatory actors, then the winner of the autonomous car race in the United States, for example, will be the one that establishes a trusted supply chain. The corporate boards, underwriters, and exchanges that address the risks of doing business with Beijing-tied partners will better be positioned to win.

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 CCTI Program

The 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.

Emily de La Bruyère is a senior fellow at FDD with a focus on China policy. Emily's work was the first Western analysis to document Beijing's China Standards 2035 national plan. She uses primary-source, Chinese-language materials to provide insight on China's military-civil fusion strategy and platform geopolitics, as well as their implications for global security and the economic order. **Nathan Picarsic** is a senior fellow at FDD with a focus on China policy. Nathan studies geopolitical and security dynamics impacting international business and finance. He has testified before the U.S.-China Economic and Security Review Commission on the risks of U.S.-China capital flows.