FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

The Risks of Chinese-Produced Cellular Modules

By RADM (Ret.) Mark Montgomery and Jack Burnham

April 2026

When a doorbell, refrigerator, or thermostat in the United States is connected to the internet, it may already be sending data to the Chinese government. These "smart" devices rely on a component known as a cellular module to connect to the internet over cellular networks. Two Chinese firms, Quectel and Fibocom, already control nearly half the global market for cellular modules. Congressional investigations and independent reporting suggest their units may pose a national security threat.[1]

Not just America's homes, but also its power grids, ports, hospitals, transportation networks, and ship-to-shore cranes increasingly rely on cellular modules. In theory, these modules can shut down their host devices in addition to collecting massive amounts of data. This is possible because manufacturers of cellular modules maintain remote access to the devices to provide software and firmware updates "over the air."[2] If Beijing consolidated control of U.S.-based modules, it could disrupt an American military mobilization in response to Chinese efforts to coerce Taiwan. Or, amid a crisis, Beijing could hold Washington hostage by threatening to cause massive economic disruption.

Dispensing with cellular modules is not an option. They are essential to automation and will be critical to integrating artificial intelligence (AI) into real-world environments, bridging the gap between frontier models and the factory floor. The challenge ahead for the United States is how to stop and reverse the proliferation of Chinese cellular modules. These risks are, so far, hypothetical, but their cumulative effects could be catastrophic.

Cellular Modules May Pose a Potent Cybersecurity Risk

With an estimated 30.9 billion devices currently deployed worldwide, cellular modules are, in effect, the backbone of the Internet of Things (IoT), an architecture that fuses disparate devices, such as drones, security cameras, port

1. House Select Committee on the CCP, Press Release, "Letter to Treasury and Defense Secretaries on 'Chinese Military Company' Quectel," January 4, 2024. (https://chinaselectcommittee.house.gov/media/letters/letter-treasury-and-defense-secretaries-chinese-military-company-quectel); House Select Committee on the CCP, Press Release, "Gallagher, Krishnamoorthi Write to FCC on Potential Risk of Chinese Internet Connectivity Modules Sabotaging Americans' Devices," August 8, 2023. (https://chinaselectcommittee.house.gov/media/press-releases/gallagher-krishnamoorthi-write-fcc-potential-risk-chinese-internet); Charles Parton, "We must face China's rare earths 2.0 moment," *FDI Intelligence*, September 16, 2025. (https://www.fdiintelligence.com/content/0e92b05f-f970-41be-aa07-c81bdc9c8895)
2. Charles Parton, "We must face China's rare earths 2.0 moment," *FDI Intelligence*, September 16, 2025. (https://www.fdiintelligence.com/content/0e92b05f-f970-41be-aa07-c81bdc9c8895)

cranes, and manufacturing tools, into centralized hubs to enable greater automation.[3] At U.S. ports, connected and remotely controlled devices accelerate offloading.[4] American power grids use networked equipment to assist in load management.[5] Hospitals need cellular modules to streamline access to electronic medical records.[6] Farms use connected devices to guide smart tractors.[7] The private-sector logistics industry has embedded cellular modules across much of its supply chain for asset tracking, management, and fleet communication. Transportation systems rely on cellular modules in traffic monitoring, connected vehicles, and the systems necessary for military mobility.[8] As firms pivot toward physical AI or combine AI with preexisting IoT infrastructure, particularly within fields such as advanced manufacturing, the cellular module market will continue to expand.[9]

Cellular modules' access to internet traffic creates a substantial surveillance risk. The modules are essential components of certain router systems, which use them to connect a Wi-Fi router to a 4G or 5G network as a form of redundancy when Wi-Fi is unavailable. Such products have become increasingly common across IoT infrastructure, particularly in industrial systems.[10] However, this feature may exacerbate security concerns since Chinese national security law allows Beijing to access firms' data to assist in state surveillance efforts.[11] Thus, China could theoretically gain access to a broad swath of Americans' information while positioning Beijing along key connectivity nodes that could be used to track specific individuals or identify broad patterns.[12]

Cellular modules are also positioned to deliver malware across the American economy. Along with importing the physical modules, American firms are also importing the proprietary software the devices run, creating the

3. "Prioritizing Security: Global Telecom's Central Emphasis in Cellular IoT Modules," *Global Telcom Engineering*, accessed February 10, 2026. (https://glob-tel.com/blog/prioritizing-security-global-telecoms-central-emphasis-in-cellular-iot-modules); Charles Parton, "Chinese cellular (IoT) modules: Countering the threat," *Council on Geostrategy*, March 19, 2024. (https://www.geostrategy.org.uk/research/chinese-cellular-iot-modules-countering-the-threat)

4. "5G At Sea: How Mobile Networks Are Transforming The Maritime Industry," *P1 Security*, July 8, 2025. (https://www.p1sec.com/blog/5g-at-sea-how-mobile-networks-are-transforming-the-maritime-industry).

5. U.S. Department of Energy, "Internet of Things-enabled Devices and the Grid," June 1, 2017. (https://www.energy.gov/articles/internet-things-enabled-devices-and-grid)

6. Hyoun-Joong Kong, Sunhee An, Sohye Lee, Sujin Cho, Jeeyoung Hong, Sungwan Kim, and Saram Lee, "Usage of the Internet of Things in Medical Institutions and its Implications," *Healthcare Information Research*, October 31, 2022. (https://pmc.ncbi.nlm.nih.gov/articles/PMC9672495)

7. Sarah Sloat, "Farmers are using IoT to take the guesswork out of growing," *Business Insider*, May 1, 2025. (https://www.businessinsider.com/iot-technology-precision-agriculture-transforming-farming-2025-5)

8. "Cellular IoT in Transportation," *IoT for All*, December 2, 2024. (https://www.iotforall.com/cellular-iot-in-transport); Annie Fixler, Mark Montgomery, and Rory Lane, "Military Mobility Depends on Secure Critical Infrastructure," *Foundation for Defense of Democracies*, March 27, 2025. (https://www.fdd.org/analysis/2025/03/27/military-mobility-depends-on-secure-critical-infrastructure)

9. John VerWey, "Physical AI: A Primer for Policymakers on AI-Robotics Convergence," *Center for Security and Emerging Technology*, February 2026. (https://cset.georgetown.edu/publication/physical-ai); Craig Singleton, Jack Burnham, and Daniel Swift, "Section 232 National Security Investigation of Imports of Robotics and Industrial Machinery," *Foundation for Defense of Democracies*, October 17, 2025. (https://www.fdd.org/analysis/2025/10/17/section-232-national-security-investigation-of-imports-of-robotics-and-industrial-machinery)

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

11. Nathan Picarsic, "Solving for Hidden Huaweis: Sector Level Approaches to Protect the US Connectivity Market," *Force Distance Times*, November 5, 2025. (https://forcedistancetimes.com/solving-for-hidden-huaweis-sector-level-approaches-to-protect-the-us-connectivity-market); Jack Burnham and Johanna Yang, "Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control," *Foundation for Defense of Democracies*, July 21, 2025. (https://www.fdd.org/analysis/2025/07/21/protecting-our-communications-networks-by-promoting-transparency-regarding-foreign-adversary-control)

12. Nathan Picarsic and Emily de La Bruyere, "Hidden Huaweis," *Real Clear Defense*, September 30, 2025. (https://www.realcleardefense.com/articles/2025/09/30/hidden_huaweis_1137911.html)

potential for them to deliver un-auditable code or malware deep into sensitive systems. This includes systems that regulate maintenance schedules, thermal management systems, and other critical processes.[13]

A more sophisticated attack could immobilize connected devices. American manufacturer John Deere revealed this type of vulnerability when it used the cellular modules in its smart tractors and other farming equipment to immobilize them after they were stolen by Russian forces in Ukraine seeking to ship them eastward.[14] This type of risk remains most prevalent within U.S. port infrastructure, with Department of Defense (DOD) officials expressing concern that Chinese cellular modules embedded in Shanghai Zhenhua Heavy Industries Company (ZPMC) cranes may both facilitate surveillance and allow Beijing to paralyze them in the event of war.[15]

China's State-Backed Campaign To Dominate the Global Cellular Module Market

Over the past two decades, Beijing has focused heavily on developing the components required to deploy its vision of the IoT both domestically and globally. As part of this effort, the Chinese Ministry of Industry and Information Technology (MIIT) designated IoT modules as a "strategic high ground" ("战略制高点之"), while the State Council identified IoT as a key emerging industry in its 12th Five-Year Plan for Strategic New Emerging Industries.[16] Along with directing state resources to build up China's cellular module sector, Beijing aims to develop a vast internal market for such technologies, having introduced a range of subsidies and trade-in programs for consumer electronics since the end of its "Zero-COVID" measures in late 2022.[17]

This support has allowed Chinese firms to win substantial market share. While still facing competition from a range of Western firms — particularly Telit Cinterion and Sierra Wireless (now part of Semtech) — Quectel and Fibocom together control nearly 45 percent of the market.

Quectel, in particular, achieved a dominant position through its aggressive lowball pricing strategy, with independent estimates suggesting that the firm sells at 15 to 20 percent below the cost of production.

Chinese firms have also purchased international competitors to bolster their hold on the market. In 2023, for example, Fibocom acquired Rolling Wireless, a European firm that developed IoT products for the automotive market, giving Beijing a greater share of Europe's IoT market.[18]

13. Francesca Ghiretti and Conlan Ellis, "It's Time to Treat China's Connected Energy Systems As a National Security Risk," *The Wire*, January 18, 2026. (https://www.thewirechina.com/2026/01/18/its-time-to-treat-chinas-connected-energy-systems-as-a-national-security-threat)

14. Emma Roth, "Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment," *The Verge*, May 2, 2022. (https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere)

15. Dustin Volz, "Espionage Probe Finds Communications Device on Chinese Cranes at U.S. Ports," *The Wall Street Journal*, March 7, 2024. (https://www.wsj.com/politics/national-security/espionage-probe-finds-communications-device-on-chinese-cargo-cranes-867d32c0)

16. Chinese Ministry of Industry and Information Technology, "物联网'十二五'发展规划 ['12th Five-Year' Plan Development Plan for the Internet of Things]," May 4, 2012. (https://digichina.stanford.edu/work/12th-five-year-development-plan-for-the-internet-sector); State Council of the People's Republic of China, "关于加快培育和发展战略性新兴产业的决定 [Decision on Accelerating the Cultivation and Development of Strategic New Emerging Industries]", October 18, 2010. (http://www.gov.cn/zwgk/2010-10/18/content_1724848.htm)

17. Daisuke Wakabayashi, "How Long Can China Keep Propping Up Its Consumers With Subsidies?" *The New York Times*, July 14, 2025. (https://www.nytimes.com/2025/07/14/business/china-economy-consumer-subsidies.html)

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

Chinese Cellular Modules Pose Operational Risks to U.S. Military Mobility

Congressional investigations have alleged that Quectel is part of Beijing's Military-Civil Fusion (MCF) strategy and reportedly tied to other MCF firms such as China Mobile and Huawei Technologies.[19] Quectel also allegedly maintains connections to China's BeiDou satellite navigation system, a core component of the PLA's precision strike capability.[20] As a result, the DOD designated Quectel as a "Chinese military company" to highlight their risk to U.S. supply chains, an action currently being contested by the firm.[21]

By exploiting the preexisting remote access that manufacturers maintain, Beijing may be in a position to disrupt a future U.S. military mobilization. Persistent monitoring could facilitate pattern-of-life analysis that Chinese intelligence might leverage to gain early indications of U.S. military movements. Beijing could also surreptitiously exploit cellular modules to collect data from cars, routers, sensors, and other devices to map sensitive locations across the United States, such as military facilities or oil and gas pipelines.

A 2024 congressional investigation warned that hundreds of ship-to-shore cranes produced by ZPMC installed in ports across the United States — including those used by the U.S. military — contained undisclosed cellular modules that China could use for espionage.[22]

In particular, China could theoretically gain insight into U.S. military operating practices, including potential access to real-time intelligence in the event of a regional military buildup. To some extent, the United States has mitigated the risk of surveillance from vehicle-mounted modules by imposing restrictions on internet-connected automotive systems produced by China.[23] Yet this, at best, addresses one facet of the challenge.

19. House Select Committee on the CCP, Press Release, "Letter to Treasury and Defense Secretaries on 'Chinese Military Company' Quectel," January 4, 2024. (https://chinaselectcommittee.house.gov/media/letters/letter-treasury-and-defense-secretaries-chinese-military-company-quectel)

20. Ibid.; John Hardie, "China, Russia Deepen Partnership on Satellite Navigation," *Foundation for Defense of Democracies*, October 20, 2022. (https://www.fdd.org/analysis/2022/10/20/china-russia-satellite-navigation)

21. Department of Defense, "Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021," January 7, 2025. (https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF); House Select Committee on the CCP, Press Release, "Gallagher, Krishnamoorthi Urge Administration to Blacklist Quectel as a 'Chinese Military Company,'" January 4, 2024. (https://chinaselectcommittee.house.gov/media/press-releases/gallagher-krishnamoorthi-urge-administration-blacklist-quectel-chinese); John Hardie, "China, Russia Deepen Partnership on Satellite Navigation," *Foundation for Defense of Democracies*, October 20, 2022. (https://www.fdd.org/analysis/2022/10/20/china-russia-satellite-navigation); "Quectel denies link to Chinese military and will fight Department of Defense Advisory Designation," *Quectel*, January 7, 2025. (https://www.quectel.com/news-and-pr/quectel-response-pentagon-1260h-list-no-military-link)

22. House Committee on Homeland Security, Press Release, "WTAS: Joint Investigation into CCP-Backed Company Supplying Cranes to U.S. Ports Reveals Shocking Findings," March 12, 2024. (https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings); Dustin Volz, "Espionage Probe Finds Communications Device on Chinese Cranes at U.S. Ports," *The Wall Street Journal*, March 7, 2024. (https://www.wsj.com/politics/national-security/espionage-probe-finds-communications-device-on-chinese-cargo-cranes-867d32c0); Aruna Viswanatha, Gordon Lubold, and Kate O'Keeffe, "Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools," *The Wall Street Journal*, March 5, 2023. (https://www.wsj.com/politics/national-security/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade)

23. Charles Parton, "Chinese cellular (IoT) modules: Countering the threat," *Council on Geostrategy*, March 19, 2024. (https://www.geostrategy.org.uk/research/chinese-cellular-iot-modules-countering-the-threat); Stephen Wilmot, "The Car Industry Is Racing to Replace Chinese Code," *The Wall Street Journal*, February 5, 2026. (https://www.wsj.com/business/autos/the-car-industry-is-racing-to-replace-chinese-code-6b939e1f?mod=author_content_page_1_pos_3)

Finally, the most critical risk associated with Chinese-produced cellular modules is their integration into the critical infrastructure essential to maintaining U.S. military mobility. Their presence opens an avenue for Beijing to sabotage U.S. forces long before they arrive at the fight. A less severe disruption might entail a "blinding" attack that limits owners' capacity to connect to their devices or prevents connected devices from functioning properly.

Recommendations

While Chinese firms hold a dominant position in the global cellular module market, the United States and its allies and partners have strong competitors and notable buying power, allowing Washington to shape the market to favor U.S. national security. By exercising this leverage through a combination of procurement bans and trade sanctions, the United States can mitigate the risks associated with Chinese cellular modules, limit their proliferation across critical infrastructure systems, and offer a positive market signal to alternative suppliers. To that end:

- **Congress should require the Department of Defense to audit its infrastructure to identify embedded Chinese cellular modules and report on associated mitigation measures.** Given their ubiquity, it is highly likely that Chinese cellular modules are embedded within DOD assets and infrastructure, including systems critical to military mobility. The department should audit its systems to gain comprehensive situational awareness of possible vulnerabilities. Once identified, the department should notify Congress of ongoing and future mitigation measures, from "rip-and-replace" programs to cycling out legacy assets.
- **Congress should ban the Department of Defense from procuring Chinese cellular modules.** Congress should mandate that DOD rely on alternative suppliers that are not subject to the jurisdiction or direction of foreign adversaries. This ban should be phased in over the course of one year, allowing the department to identify alternative contractors.
- **The Federal Communications Commission (FCC) should add Chinese cellular module manufacturers to its Covered List.** While they are integrated into a range of consumer products, cellular modules are fundamentally communications devices that rely on the U.S. cellular network to provide connectivity. The FCC should ensure that Chinese firms with ties to Beijing are added to the Covered List, restricting the sale of their products in America.

Conclusion

Chinese cellular modules present a clear and present national security risk to the United States. They offer Beijing an avenue to amplify its espionage campaigns and potentially disrupt critical infrastructure that underpins both U.S. economic prosperity and military mobility. As Chinese firms aim to consolidate their hold over this critical market, the U.S. government has a limited window to safeguard defense-critical operations and promote secure supply chains by enacting procurement bans and limiting its adversary's market access.

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

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.

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.

RADM (Ret.) Mark Montgomery serves as senior director of FDD's Center on Cyber and Technology Innovation and an FDD senior fellow. Mark served 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017. His flag officer assignments included director of operations (J3) at U.S. Pacific Command; commander of Carrier Strike Group 5 aboard the USS *George Washington* in Japan; and deputy director for plans, policy, and strategy (J5) at U.S. European Command. From 1998 to 2000, he served at the National Security Council as director for transnational threats.

Jack Burnham is a senior research analyst at FDD's China Program. His research primarily focuses on China's military, emerging technologies, and science and technology policy. He also researches and analyzes the role of innovative technology in changing the character of contemporary conflict. Jack earned a master's in public policy from the Max Bell School of Public Policy at McGill University and a B.A. with honors in political studies from Queen's University.
