

Federal Communications Commission

Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control

Docket No. 47 CFR Parts 1, 2, 13, 15, 17, 22, 24,
25, 26, 27, 30, 52, 54, 63, 64, 73, 76, 80, 87, 88, 90,
95, 96, 97, 101 [GN Docket No. 25-166; FCC 25-28;
FR ID 299066]

AUTHORS

Jack Burnham

Research Analyst, FDD's China Program

Johanna Yang

*Research and Editorial Associate, FDD's
Center on Cyber and Technology
Innovation*

Washington, DC
July 21, 2025

Introduction

China's far-reaching intrusion into U.S. communications networks and associated sectors poses a clear and present danger to U.S. national security. Seeking to surpass the United States as the world's leading power, the Chinese Communist Party (CCP) has launched an extensive effort to conduct espionage, pre-position cyber assets within U.S. critical infrastructure, and infiltrate the American market.

To counter this threat, the Federal Communications Commission (FCC) must strengthen its approach to preventing foreign adversaries from owning key aspects of the nation's communications network. While the FCC has targeted select sectors for greater scrutiny, such as equipment testing laboratories and submarine cables, these measures have not extended to other FCC-regulated markets, leaving an opening for the CCP to expand its influence. Moreover, the FCC's foreign ownership regulations remain limited and fail to address common pathways for the CCP to exercise control over Chinese firms, such as national security regulations and opaque corporate governance structures.

China's growing ambition to dominate the global telecommunications market has manifested across a range of industries, from drones to submarine cables. Spurred by aggressive industrial policies such as Made in China 2025, Beijing has poured resources into becoming a global leader in science and technology, by innovating or stealing key breakthroughs and using its vast manufacturing capacity to add weight to its advances.¹ This practice has given China expansive leverage over several key markets, either fully or partially regulated by the Commission, including drones connected to U.S. networks, telecommunications and broadband infrastructure, undersea communications cables, and equipment-testing laboratories.

Moreover, China has constructed the domestic legal and regulatory architecture necessary to weaponize these advantages. China's 2017 National Intelligence Law — along with other legal instruments — mandates that Chinese firms and individuals under Beijing's jurisdiction cooperate with intelligence officials and other state authorities, blurring the line between commerce and coercion.² The CCP's embrace of a policy of military-civil fusion (MCF) has further blurred these lines, with major Chinese civilian firms forced into collaboration with defense contractors, ensuring that cutting-edge civilian innovation fuels the country's

¹ Emily de La Bruyère, "Made in China 2025—Who Is Winning?" *Foundation for Defense of Democracies*, February 6, 2025. (<https://www.fdd.org/analysis/2025/02/06/made-in-china-2025-who-is-winning>); "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," *Xinhua News Agency*, March 12, 2021. (archived version available at <https://perma.cc/73AKBUW2>)

² Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024. (<https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems/>)

unprecedented military build-up.³ Products from major Chinese firms have also been integrated into the Commission's equipment testing process, potentially allowing security vulnerabilities to enter the American market.⁴

In response, the FCC should institute several measures to screen Chinese entities looking to enter the U.S. telecommunications market:

The Federal Communications Commission (FCC) should broaden the scope of its foreign ownership reporting requirements to cover all applicants for licenses, permits, and other authorizations. This expansion will streamline efforts to prevent China and other foreign adversaries from accessing the nation's telecommunications network, while preventing states, entities, and individuals from circumventing reporting requirements.

The FCC should also expand the definition of foreign ownership to include entities controlled by, or subject to, the jurisdiction or direction of a foreign adversary. This expansion will stymie Beijing's efforts to use its regulatory and legal architecture to coerce nominally independent firms into furthering the CCP's geopolitical ambitions. This comment will provide further detail of the threat posed by Chinese involvement in the U.S. telecommunications sector.

Overview of the Threat From Firms Under the Jurisdiction of Foreign Adversaries (the People's Republic of China)

China's extensive legal and regulatory architecture, coupled with its role as a key node within U.S. supply chains, poses a direct threat to a range of FCC-regulated markets, including foreign equipment entering the United States, the nation's telecommunications infrastructure, and sectors crucial for national security, such as submarine cables.

China's National Security Law, National Intelligence Law, and Cybersecurity Law facilitate Chinese authorities' access to information collected by firms and individuals subject to Beijing's jurisdiction, effectively blurring the lines between commercial ventures and intelligence collection.⁵ This issue is only heightened by the CCP's reliance on other mechanisms to control

³ Emily de La Bruyère and Nathan Picarsic, "Defusing Military-Civil Fusion," *Foundation for Defense of Democracies*, May 27, 2021. (<https://www.fdd.org/analysis/2021/05/26/defusing-military-civil-fusion>)

⁴ Mark Montgomery and Jiwon Ma, "Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program," *Foundation for Defense of Democracies*, April 14, 2025. (<https://www.fdd.org/analysis/2025/04/14/promoting-the-integrity-and-security-of-telecommunications-certification-bodies-measurement-facilities-and-the-equipment-authorization-program/>)

⁵ Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024.

private firms, such as seizing “golden shares” and placing party cadres in key roles to direct corporate strategy.

Along with blurring the lines between intelligence collection and commercial expansion, Beijing continues to pursue MCF, seeking to combine the country’s defense industrial base with its burgeoning high-tech economy. While MCF began in 2007, Chinese paramount leader Xi Jinping has transformed these efforts into a flagship state policy to spur military modernization and funnel commercial-relevant innovation to Chinese firms, including telecommunications providers, unmanned aircraft systems (UAS) firms, and other segments of the domestic economy.⁶

China has also relied on its firms’ involvement over key aspects of FCC policymaking to circumvent scrutiny, particularly Telecommunications Certification Bodies (TCBs) and Measurement Facilities (labs). These organizations assess the safety of consumer products entering the U.S. market to ensure their compliance with FCC regulations. Chinese firms, including those connected to the People’s Liberation Army (PLA) and the CCP, have participated in these reviews, collectively accessing thousands of consumer products destined for the U.S. market.⁷

This legal and regulatory architecture allows Beijing to translate its firms’ commercial dominance across a range of industries into a weapon to achieve its geopolitical ambitions. China’s dominance of the American UAS supply chain — from completed products to key components such as flight controllers, software, and gyroscopes — allows Beijing to exercise significant control over the U.S. drone market.⁸ Beijing leverages this influence in pursuit of its geopolitical ambitions, limiting American drone manufacturer Skydio’s access to Chinese batteries due to its sales to Taiwan and allegedly installing backdoor access into common flight controller applications.⁹

(<https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems>)

⁶ Emily de La Bruyère and Nathan Picarsic, “Defusing Military-Civil Fusion,” *Foundation for Defense of Democracies*, May 27, 2021. (<https://www.fdd.org/analysis/2021/05/26/defusing-military-civil-fusion>); Jack Burnham, Johanna Yang, “Chinese Leader Xi Jinping Calls for Greater Local Support for Military Modernization,” *Foundation for Defense of Democracies*, March 13, 2025.

(https://www.fdd.org/analysis/policy_briefs/2025/03/13/chinese-leader-xi-jinping-calls-for-greater-local-support-for-military-modernization/)

⁷ U.S. Federal Communications Commission, “Fact Sheet: FCC Voting This Week on Proposal to Ban ‘Bad Labs’,” May 21, 2025, page 1. (<https://docs.fcc.gov/public/attachments/DOC-402704A1.pdf>)

⁸ Mark Montgomery, Craig Singleton, Johanna Yang, Jack Burnham, “Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems,” *Foundation for Defense of Democracies*, March 4, 2025. (<https://www.fdd.org/wp-content/uploads/2025/03/FDD-UAS-Comment.pdf>)

⁹ Jack Burnham, “President Trump Issues Executive Orders to Counter China’s Drone Industry,” *Foundation of Defense of Democracies*, June 10, 2025. (https://www.fdd.org/analysis/policy_briefs/2025/06/10/president-trump-issues-executive-orders-to-counter-chinas-drone-industry/); Mark Montgomery, Craig Singleton, Johanna Yang, Jack

Chinese dominance of the UAS information and communication technology and services (ICTS) supply chain also poses significant surveillance and sabotage concerns. From mapping military and critical infrastructure installations to collecting user data and servicing sensitive sectors such as agriculture, China's market position offers significant opportunities for both espionage and sabotage.

This threat extends to America's telecommunications network, as Beijing has continued to leverage its advanced cyber capabilities to identify vulnerabilities within U.S. infrastructure and pre-position destructive assets in the event of a crisis. While China has long used cyber campaigns to steal U.S. intellectual property and proprietary government data, Beijing has increasingly adopted a posture of operational preparation of the battlefield — identifying key networks crucial for societal continuity, locating vulnerabilities, and preparing sabotage options.¹⁰

This shift in posture comes as China has launched a series of cyber-enabled espionage and sabotage campaigns. These include "Salt Typhoon," which allowed Beijing unprecedented access into U.S. telecommunications networks, including the communications of senior U.S. government officials; "Volt Typhoon," which gave Chinese hackers access to water, electricity, and critical infrastructure; and "Flax Typhoon," which included Chinese penetration into communication networks between the United States and Taiwan.¹¹

These cyberattacks appear to have been partially enabled by Chinese-manufactured router equipment entering the U.S. market, particularly TP-Link equipment. Despite being one of the largest suppliers of router equipment in the United States, TP-Link has been accused by Microsoft and other U.S. intelligence agencies of hiding security vulnerabilities within its products.¹² These concerns, compounded by TP-Link's alleged unfair market practices, have led Congress to pressure the Department of Commerce to ban its products from entering the U.S. market.

Burnham, "Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems," *Foundation for Defense of Democracies*, March 4, 2025. (<https://www.fdd.org/wp-content/uploads/2025/03/FDD-UAS-Comment.pdf>)

¹⁰ Mark Montgomery, "Unconstrained Actors," *Testimony before the House Committee on Homeland Security*, January 22, 2025. (<https://www.fdd.org/analysis/2025/01/22/unconstrained-actors-assessing-global-cyber-threats-to-the-homeland/>)

¹¹ Mark Montgomery, Craig Singleton, Johanna Yang, Jack Burnham, "Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems," *Foundation for Defense of Democracies*, March 4, 2025. (<https://www.fdd.org/wp-content/uploads/2025/03/FDD-UAS-Comment.pdf>)

¹² Joe Supan, "TP-Link Is Under Investigation for Predatory Pricing. Should You Replace Your Router?" *CNET*, May 1, 2025. (<https://www.cnet.com/home/internet/tp-link-is-under-investigation-for-predatory-pricing-should-you-replace-your-router/>)

China's reach into FCC-regulated infrastructure also extends to undersea communications cables, which directly underpin the nation's economic vitality and military command and control structures. Having identified submarine cable infrastructure as an essential component of economic growth, China has ramped up its efforts to expand both its manufacturing capacity and its role as a key operator of cable infrastructure.¹³ Chinese firms are key suppliers of optical and power components for undersea repeaters, while state-owned companies such as China Telecom and China Unicom have built out control over key markets within the Middle East and Southeast Asia.¹⁴ China also operates a substantial fleet of undersea cable repair vessels, providing Beijing with a potent dual-use capability to interrupt U.S. submarine cable traffic during a military crisis.¹⁵

Recommendations to Strengthen the Cyber-Physical Resilience of the U.S. Telecommunications Sector

To safeguard U.S. national security, the Commission should expand foreign ownership disclosure requirements for all licenses, applications, and other issued certifications while broadening its definition of foreign ownership to encompass firms subject to, or under the jurisdiction of, a foreign adversary.

- **The Commission should adopt its proposed disclosure requirements across various licenses, authorizations, permits, and other approvals regulated by the Commission.** China continues to target a broad range of FCC-regulated sectors, including telecommunications, broadband, equipment, certification regimes, and submarine cables. While the intensity of the CCP's efforts has varied from sector to sector, enacting a broad set of requirements will fully protect U.S. national security while proactively guarding against future threats.

¹³ Lane Burdette, "Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy," *Journal of Public and International Affairs*, May 5, 2021. (<https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>)

¹⁴ Justin Sherman, "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security," Atlantic Council, September 2021. (<https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/>); Mark Montgomery, Craig Singleton, Jack Burnham, Annie Fixler, "Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Schedule of Application Fees," *Foundation for Defense of Democracies*, April 14, 2025. (<https://www.fdd.org/analysis/2025/04/14/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security-law-enforcement-foreign-policy-and-trade-policy-risks-schedule-of-application-fees/>)

¹⁵ Micah McCartney, "China Unveils Game-Changing Weapon That Could Decide Future Wars," *Newsweek*, March 24, 2025. (<https://www.newsweek.com/china-unveils-game-changing-weapon-that-could-decide-future-wars-2049477>)

- **The Commission should adopt a “dominant minority” definition in relation to equity and voting interests.** Beijing uses a range of corporate governance structures, including “golden shares,” shell companies, and other intermediaries, to obscure its control over both Chinese and foreign-domiciled firms. This definition will effectively capture these dynamics within the regulatory process.
- **The Commission should expand its definition to include “controlling interests” that go beyond equity and voting interests.** The Commission should consider other corporate governance structures in considering a firm’s ties to a foreign adversary, particularly given China’s exploitation of alternative governance structures to exercise control over nominally commercial ventures.
- **The Commission should adopt a standard 5 percent threshold for ownership and control regulations.** The Commission should adopt a lower threshold for determining foreign ownership and control due to China’s reliance on shell companies and other forms of corporate governance intended to circumvent regulatory scrutiny.
- **The Commission should expand sourcing for its list of “foreign adversaries” to include the Consolidated Screening List and other designations.** Along with its current Covered List, the Commission should also rely on the Consolidated Screening List, a list of parties for which the U.S. government maintains restrictions on exports, re-exports, or the transfer of items. In determining its list of “foreign adversaries,” the Commission should also rely on the Entity List maintained by the Bureau of Industry and Security and the 1260H List maintained by the Department of Defense.
- **The Commission should require additional information from regulated entities with reportable foreign adversary control.** The Commission should require firms or individuals under its regulatory jurisdiction to report on their interactions with a foreign adversary government, including its officials or officers of its dominant political party. The Commission should also require these regulated entities to submit to standard questions as part of the executive branch review process. This process should also force regulated entities to report on interactions within the United States, particularly on contracts with U.S. entities, products and services, and their interactions with U.S. communications networks.
- **The Commission should require regulated entities to inform the Commission of any deficiencies in complying with its requests to solicit information regarding their relationships with foreign adversaries.** The Commission should be required to send a letter to request explanations or corrections from regulated entities; a failure to comply

within 30 days should result in the Commission automatically revoking the regulated entities' covered authorization.

Conclusion

The CCP's efforts to infiltrate and disrupt America's communications infrastructure pose a direct threat to U.S. national security. The FCC's proposed expansion of foreign ownership disclosure requirements across all its licenses, authorizations, and permits is a necessary and appropriate step to counter Chinese malign activity within the nation's communications industry. Moreover, the FCC's proposed definition of foreign ownership to include firms under foreign adversarial control will stymie the CCP's efforts to circumvent the Commission's regulatory oversight.

Thank you for considering our comments, and we look forward to seeing how our input is incorporated into the final rule.