PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

FEDERAL COMMUNICATIONS COMMISSION

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

47 CFR Parts 0, 1, and 43

OI Docket No. 24-523, MD Docket No. 24-524

AUTHORS

RADM (Ret.) Mark Montgomery
Senior Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Craig Singleton
Senior Director of the China Program at the Foundation for Defense of Democracies

Jack Burnham
Research Analyst for the China Program at the Foundation for Defense of Democracies

Annie Fixler
Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Washington, DC
April 14, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Relying on its extensive network of state-directed industries and backed by intrusive surveillance laws, the Chinese Communist Party (CCP) has sought to seize control of submarine cables, the backbone of the global communications network, to fulfill its long-term geopolitical ambitions and undermine U.S. national security.

Supported by its investments in global communications networks under the auspices of the Belt and Road Initiative (BRI), Chinese submarine cable producers and operators have rapidly gained a significant global market share.[1] Backed in part by state investments, Beijing has continued to launch increasingly advanced cable maintenance vessels, which can also be used to damage or disrupt undersea infrastructure.[2]

China's growing capabilities have fueled its emerging role as a key player within undersea cable production, introducing vulnerabilities into critical U.S. supply chains and threatening to undermine U.S. economic and national security. These risks are heightened by China's sweeping national security laws, which mandate that firms operating within Beijing's jurisdiction collaborate with intelligence-gathering operations and other surveillance campaigns.

Beijing has paired efforts to dominate the undersea cable industry with escalatory use of cyberattacks to conduct espionage and pre-position destructive and disruptive capabilities on U.S. critical infrastructure. Chinese state-sponsored hacking campaigns known as Salt Typhoon, Volt Typhoon, and Flax Typhoon have compromised U.S. telecommunications networks, infiltrated U.S. critical infrastructure systems, and penetrated communications networks between the mainland United States and Taiwan.[3] Along with gaining valuable intelligence, these

---

[1] 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)

[2] Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," *Center for Strategic and International Studies*, August 16, 2024. (https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition); 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)

[3] Craig Singleton, "China's Tech Triple Play Threatens U.S. National Security," *Real Clear Defense*, March 25, 2025. (https://www.realcleardefense.com/articles/2025/03/25/chinas_tech_triple_play_threatens_us_national_security_1099692.html); Jack Burnham, "Chinese-Linked Hackers Accused of Infiltrating U.S. Treasury Department," *Foundation for Defense of Democracies*, January 3, 2025. (https://www.fdd.org/analysis/policy_briefs/2025/01/03/chinese-linked-hackers-accused-of-infiltrating-u-s-treasury-department)

campaigns signal that China is currently conducting operational preparation of the battlefield in advance of a possible military crisis between Washington and Beijing.[4]

China's rapid rise as both a producer and operator of submarine cables poses a distinct danger to U.S. national security. Submarine cables carry nearly 95 percent of global internet traffic, including commercial transactions, government services, and civilian communications, while military cables are critical for maintaining command-and-control systems.[5] The introduction of Chinese components or ownership of U.S. submarine cable infrastructure by Chinese state-owned enterprises will dramatically heighten the risk of espionage or sabotage.

The Federal Communications Commission (FCC) should prohibit any entity on the Covered List, along with those subject to the jurisdiction, direction, or control of a foreign adversary, from owning submarine cables connected to the United States. These restrictions will both ensure that Chinese state-owned firms cannot exercise control over submarine cable infrastructure and prevent the CCP from relying on nominally private civilian firms to advance its geopolitical ambitions.

The FCC should also restrict submarine cable manufacturers from incorporating equipment from firms on the Covered List, along with components produced by firms under the jurisdiction of foreign adversaries. This regulation will prevent Beijing from using its control over strategic supply chains to introduce vulnerabilities into a key pillar of U.S. critical infrastructure.

This comment will provide further detail into the threat posed by Chinese involvement in the U.S. submarine cable sector.

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

Having identified the United States as the primary obstacle to its rise as a superpower, Beijing has worked to leverage all facets of national power, particularly its economic and military strength, to degrade Washington's global standing.

The CCP expects Chinese private firms to serve the party's interlocking interests of delivering economic growth while contributing to national security. Despite their nominal independence

[4] Mark Montgomery, Craig Singleton, Johanna Yang, and 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.regulations.gov/comment/BIS-2024-0058-0496)
[5] Colin Wall and Pierre Morcos, "Invisible and Vital: Undersea Cables and Transatlantic Security," *Center for Strategic and International Studies*, June 11, 2021. (https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security)

from Beijing, Chinese firms, including those operating abroad while remaining subject to Chinese jurisdiction, are subject to a series of strict national security regulations. These regulations, particularly the 2015 National Security Law, the 2017 National Intelligence Law, and the 2021 Data Security Law, allow the CCP to gain access to information collected by Chinese firms while mandating cooperation with state surveillance efforts.[6] Beyond its regulatory regimes, the party also uses a variety of ownership structures, including "golden shares," to exert direct influence over select private firms and their subsidiaries without entering traditional ownership arrangements.[7] This permissive legal environment ensures that even nominally private firms subject to Beijing's jurisdiction may be drafted by the CCP to further its interests.

These legal efforts complement more direct measures of CCP intrusion into the Chinese economy, namely the party's pursuit of military-civil fusion (MCF). Introduced in 2007, MCF intends to integrate China's civilian economy into its defense industrial base, allowing for the military to rapidly adopt civilian innovations while simultaneously supporting the rise of China's technology sector.[8] Under the tenure of General Secretary Xi Jinping, MCF has rapidly expanded to incorporate a broad range of technology firms, advanced manufacturers, telecommunications providers, and other sectors of the country's domestic economy.[9] By linking China's high-tech sector to its military industrial base, the CCP has effectively blurred the lines between civilian firms and defense contractors, raising the risk of Chinese firms being directed to commit acts of espionage and sabotage within U.S. critical infrastructure.

Evaluation of the Risk Posed by Chinese Involvement in the U.S. Submarine Cable Supply Chain

The implications of the CCP's use of civilian firms to achieve its national security ambitions extend to its role within critical supply chains for submarine cables and adjacent industries and services. Having sought to expand its influence across much of Southeast Asia and into the broader Gulf region, China has aggressively supported its domestic submarine cable industry via

---

[6] 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)

[7] Lingling Wei, "China's New Way to Control Its Biggest Companies: Golden Shares," *The Wall Street Journal*, March 8, 2023. (https://www.wsj.com/articles/xi-jinpings-subtle-strategy-to-control-chinas-biggest-companies-ad001a63)

[8] 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)

[9] Jack Burnham and 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)

financing purchases for its broader Belt and Road Initiative (BRI).[10] These purchases have allowed Chinese firms such as HMN Technologies, previously owned by Huawei, and ZTT Group to expand their holdings within the global marketplace while establishing relationships with potential U.S. customers.[11] Along with supporting major suppliers, Chinese state-owned cable operators such as China Telecom and China Unicom also operate crucial communications networks, particularly among lower-resource countries.[12]

This global growth strategy is reflective of Beijing's broader efforts to weaponize chokepoints within critical communication supply chains in order to extend its leverage over the United States and its allies and partners. Under "Made in China 2025" (the CCP's state-sponsored industrial policy) and the 14th Five-Year Plan, Beijing has sought to build up its advanced manufacturing base to gain leverage over global value chains while undercutting foreign competitors.[13] These efforts have allowed China to dominate the production of key components for submarine cables, including optical and power components for undersea repeaters.

Beijing has also sought to translate its leverage over global supply chains into avenues to pursue espionage and sabotage campaigns against Washington and its allies and partners. Having recognized the role of submarine cables in carrying both civilian and military communications, China has unveiled a series of cable-laying and repair vessels, both of which also present dual-use capabilities to interrupt U.S. and allied communications during a possible military crisis.[14]

Beijing has also repeatedly demonstrated its willingness to use security gaps within U.S. critical infrastructure to conduct espionage and pre-position malicious cyber measures (malware) designed to produce societal chaos and disrupt U.S. military operations. Along with conducting espionage, including monitoring communications between high-level government personnel and

---

[10] 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); Dale Aluf, "China's Subseacable Power Play in the Middle East and North Africa," *Atlantic Council*, May 2023. (https://www.atlanticcouncil.org/wp-content/uploads/2023/05/ChinasGrowingInfluence_052423-1.pdf)

[11] Sadia Rahman, "The Cable Ties to China's Digital Silk Road," *The Lowy Institute*, April 29, 2024. (https://www.lowyinstitute.org/the-interpreter/cable-ties-china-s-digital-silk-road); Sam Clark, "The West Has a Plan to Keep China, Russia Out of Subsea Data Pipes," *Politico*, September 12, 2024. (https://www.politico.eu/article/china-russia-submarine-data-cables-security-united-states-european-union)

[12] Justin Sherman, "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security," *Atlantic Council*, September 2021. (https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf)

[13] 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/73AK-BUW2)

[14] 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)

mapping critical infrastructure, Beijing has also used its control over supply chains to sabotage U.S. firms and target systems critical for military mobility.[15] These risks are heightened by private firms' use of remote network management systems, particularly those connected directly to the internet, to control submarine cable systems.

Recommendations to Strengthen the Cyber-Physical Resilience of U.S. Submarine Cable Infrastructure

In addition to prohibiting Chinese ownership of submarine cables and the integration of Chinese components into existing infrastructure, the FCC should take the following steps to bolster the resilience of submarine cable infrastructure through cybersecurity requirements, ownership transparency, and physical security standards.

1. **The commission should prohibit any entity on the Covered List, along with those subject to the jurisdiction, direction, or control of a foreign adversary, from owning submarine cables connected to the United States.** These restrictions will prevent Chinese state-owned or state-aligned firms from exercising control over submarine cable infrastructure.

2. **The FCC should restrict submarine cable manufacturers from incorporating equipment from firms on the Covered List, along with components produced by firms under the jurisdiction of foreign adversaries.** This regulation will prevent Beijing from using its control over strategic supply chains to introduce vulnerabilities into submarine cable infrastructure.

3. **The FCC should strengthen the cybersecurity requirements of submarine cable owners and licensees to mitigate Chinese intrusions.** These measures should require (1) all applicants/licensees to report or certify that they have created, updated, and implemented cybersecurity risk management plans consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, (2) third-party cybersecurity vendors used by applicants/licensees to submit cybersecurity risk management plans, and (3) applicants/licensees to maintain such documentation for up to two years.

[15] Craig Singleton, "China's Tech Triple Play Threatens U.S. National Security," *Real Clear Defense*, March 25, 2025. (https://www.realcleardefense.com/articles/2025/03/25/chinas_tech_triple_play_threatens_us_national_security_1099692.html); 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)

4. **The FCC should also require cable owners and licensees to disclose ownership of cable landing stations and associated infrastructure**. As part of its rulemaking process, the FCC should expand its transparency requirements for entities seeking to obtain a license or access U.S. submarine cable infrastructure. Applicants for licenses should be required to divulge whether they will be using foreign-owned Managed Network Service Providers (MNSPs). Applicants that use foreign-owned MNSPs should be screened using the FCC's MNSP Standard Questions. The FCC should refer those applications to relevant executive branch agencies. This mechanism will ensure that the FCC can monitor a key avenue for foreign firms or individuals to access submarine cable infrastructure. This screening mechanism should extend to any entity or individual, whether foreign or domestic, that maintains logical access to the submarine cable system. Additionally, the FCC should consider mandating that both foreign and domestic entities with either ownership or indirect control over cable landing stations or submarine line terminal equipment be listed on licensing documents.

5. **These measures should also be bolstered by stronger physical security standards and disclosures.** The FCC should require license applicants, regardless of foreign ownership, to list anticipated or actual physical addresses for their network operations centers, along with coordinates for beach manholes and cable landing stations. All applicants should also be required to list the locations of key aspects of their proposed or current cable system, including landing points, the number of segments and their respective typology, the location of branching units, the number of fiber optic pairs by segment, the design capacity of each segment, and a timeline for deployment. While extensive, this information is critical to safeguarding submarine cables by preventing accidental damage from other maritime activities and monitoring the activities of adversarial state actors.

6. **These physical security regulations should be paired with broader efforts to protect cable landing stations from physical threats and natural disasters**, including reinforcing infrastructure against intense weather events and investing in surveillance capabilities to monitor access points. The FCC should consider establishing cable protection zones to limit activity that could pose a risk of cable damage. The FCC should also explore more robust, scalable sensors and data analysis to detect threats faster.

Conclusion

The CCP's efforts to dominate and disrupt U.S. and global submarine cable infrastructure pose a direct threat to U.S. national security. The FCC's proposed regulation to limit foreign ownership of submarine cables by firms under the jurisdiction of adversarial countries, prohibit the installation of components produced by foreign adversary companies, and strengthen

cybersecurity and physical security measures are absolutely appropriate and critical to protecting the United States from espionage and sabotage.

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