

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

47 CFR Part 1

[OI Docket No. 24-523, MD Docket No. 24-524; FCC 25-49; FR ID 311053]

AUTHORS

Jack Burnham

Research Analyst, FDD's China Program

RADM (Ret.) Mark Montgomery

Senior Director and Fellow, FDD's Center on Cyber and Technology Innovation

Craig Singleton

Senior Director and Senior Fellow, FDD's China Program

**Washington, DC
November 20, 2025**

Introduction

China's growing ambitions within the submarine cable sector have introduced vulnerabilities into critical U.S. supply chains, threatening to undermine U.S. economic and national security. Submarine cables carry nearly 95 percent of global internet traffic, including commercial transactions, government services, and civilian communications. They are also critical for maintaining military command-and-control systems.¹

Chinese submarine cable producers and operators have rapidly gained a significant global market share, particularly in Southeast Asia and the Middle East, controlling an ever-growing percentage of the global communications networks under the auspices of the Belt and Road Initiative (BRI). At the same time, Beijing has launched increasingly advanced cable maintenance vessels, which can also be used to damage or disrupt undersea infrastructure.

This risk is emerging just as the Chinese Communist Party's (CCP's) state-sponsored hacking campaigns, such 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.² Moreover, Chinese cable providers, operating under Beijing's jurisdiction, remain subject to China's sweeping national security laws, including a mandate to collaborate with intelligence-gathering operations and other surveillance campaigns.

This comment will provide further detail on the threat posed by Chinese involvement in the U.S. submarine cable sector and offer several recommendations to the Federal Communications Commission (FCC) to safeguard national security.

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

China has aggressively attempted to dominate the submarine cable market — a move that poses long-term national security risks to 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

¹ Mark Montgomery, Craig Singleton, Jack Burnham, and 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>)

² 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)

while undercutting foreign competitors.³ The CCP has expanded this support to China's domestic submarine cable industry, primarily via financing for purchases from domestic firms to support Beijing's broader Belt and Road Initiative (BRI). Chinese state-owned cable operators such as China Telecom and China Unicom operate crucial communications networks for a range of private and government customers, particularly in lower-resource countries. This market presence has also allowed Chinese firms such as HMN Technologies, previously owned by Huawei, and ZTT Group to expand their cable holdings within the global marketplace while establishing relationships with potential U.S. customers, particularly for key components such as optical and power components for undersea repeaters.⁴

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 with dual-use capabilities to cut U.S. and allied communications during a possible military crisis.⁵ These efforts operate in conjunction with Beijing's expanded cyber campaigns against the United States, including monitoring communications between high-level government personnel, mapping critical infrastructure, and sabotaging U.S. firms and systems critical for military mobility.⁶ Combined, these efforts may allow China to wreak havoc in critical infrastructure systems by either interfering with undersea cables that protect American interests or undermining third-party technologies, such as remote network management systems directly connected to the internet.

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

In addition to prohibiting Chinese ownership of submarine cables landing on the United States and the integration of Chinese components into existing infrastructure, the Federal Communications Commission should take the following steps to bolster the resilience of

³ 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>); "中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 [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>)

⁴ Mark Montgomery, Craig Singleton, Jack Burnham, and 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>)

⁵ 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>)

⁶ 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>)

submarine cable infrastructure through cybersecurity requirements, ownership transparency, and physical security standards.

Prioritizing Sensible National Security Considerations for Proposed Submarine Line Terminal Equipment Blanket Licenses

- **Any entity that owns or operates submarine line terminal equipment (SLTE) should be mandated to become a license holder.** This approach will ensure that any entity that has a significant stake in the construction, operation, maintenance, and continuity of submarine cables falls under the Commission's jurisdiction and becomes subject to critical national security regulations. However, to reduce the burden on regulated entities, this license should cover both owners and operators, streamlining the regulatory process by avoiding potentially duplicative actions without compromising the FCC's regulatory authority or generating any oversight gaps.
- **Under the auspices of safeguarding national security, the FCC should exclude certain entities from obtaining a blanket license.** The Commission should block any entity subject to or controlled by a foreign adversary from owning or operating any current or new SLTEs that land on the United States. Beyond offering a balance between streamlining licensing to ease industry concerns and safeguarding national security, this measure will also allow the FCC to effectively utilize its regulatory authority to isolate specific entities for greater scrutiny.
- **The FCC should mandate that both current and future licensees comply with strict security regulations.** The FCC should ensure that all applicants and current owners and operators develop and deploy robust security standards, particularly related to natural disaster preparedness, Covered List compliance, and foreign adversary-related disclosures and prohibitions. These standards should be aimed at ensuring the continuity of the economy in the event of a crisis, along with deterring adversarial nation-states, such as China, from accessing or damaging submarine cable infrastructure using a range of physical or cyber-related measures.
- **The FCC should require all licensees to file an SLTE Foreign Adversary Annual Report.** This report should include information about the SLTE owner and operator, the location of the SLTE, and whether the SLTE owner or operator sells, shares, or swaps fiber or spectrum on a licensed submarine cable system. This report will enhance the Commission's oversight over the nation's submarine cable system and assist in identifying potential adversarial intrusions or interference.

Ensuring Executive Branch Oversight of Submarine Cable Applications

- **The FCC should adopt a stringent national security standard for submarine cable applications, including applications for landing licenses, assignment, transfer of control, or renewal and extension.** These should include, at minimum, requirements to report all individuals and entities under the control or subject to the jurisdiction or direction of a foreign adversary that holds a five-percent-or-more stake of an applicant;

and whether the applicant currently plans to or currently uses any equipment on the Covered List. This information should also include the use of any third-party service providers that maintain remote access and the status of their physical and cybersecurity implementation plans. If an applicant answers affirmatively in reporting foreign ownership or the other requested information is deemed insufficient, their applicant should be reviewed by relevant Executive Branch agencies.

Incentivize and Encourage the Adoption and Use of Trusted Technologies Produced and Provided by the United States and its Foreign Allies

- **The FCC should not grant licenses to entities that use any equipment produced by an entity controlled or subject to the jurisdiction or direction of a foreign adversary.** This standard should apply to all equipment, not just logic-bearing hardware or software or communications equipment, given previously identified vulnerabilities across a range of components produced by foreign adversaries and China's continuous efforts to utilize vulnerabilities across every aspect of the supply chain. This measure will also complement the FCC's current actions on decertifying equipment testing laboratories controlled by foreign adversaries.
- **The FCC should mandate that licensees certify any new editions of equipment or services on the Covered List.** The Commission should use its regulatory authority to deter or prevent new licensees from adopting any equipment on the Covered List, while the FCC should also mandate that all licensees, regardless of when they have received their license, report any Covered List items within their systems. This measure will offer the FCC improved insight into the submarine cable sector and assist in determining potential security vulnerabilities.
- **The FCC should prohibit the use of certain third-party service providers.** The Commission should prohibit any landing license holder (licensed for cables that land on U.S. shores) from using any third-party service provider under the control or subject to the jurisdiction or direction of a foreign adversary. The FCC should also prevent the use of any third-party services from an entity on the Covered List, or an entity that can access the cable or requisite components from a foreign adversarial country.
- **The FCC should promote U.S. and allied-built repair ship construction.** Within its defined regulatory role, the Commission should facilitate the revitalization and rebuilding of domestic maritime industries and allied-built shipping. Though not exclusive, these efforts should prioritize maximizing current investments by U.S. allies, particularly South Korea and Japan, in American shipyards, incentivizing the transfer of technical expertise and advanced construction methods.

Conclusion

Beijing'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 regulations are both 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.