PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Federal Communications Commission

2022 Quadrennial Regulatory Review-Review of the Commission's Broadcast Ownership Rules and Other Rules Adopted Pursuant to the Telecommunications Act of 1996

47 CFR Part 73

[MB Docket No. 22-459; FCC 25-64; FR ID 317689]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

Jiwon Ma
Senior Policy Analyst, FDD's Center on Cyber and Technology Innovation

Washington, DC
December 17, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

America's national communications infrastructure is a key strategic asset and will likely be a center of gravity of any adversarial campaign targeting the United States, making its protection a national security priority. The United States has a broad, diverse set of communications channels, yet the national reach of these mediums faces increasing challenges from both market dynamics and adversarial activity.

Radio, including professional broadcasters and amateur shortwave, remains crucial within rural regions and local broadcast television is a trusted source of information for most Americans.[1] However, both radio listenership and broadcast television viewership have declined significantly due to the rise of streaming services. This shift inadvertently places key information-sharing systems at an increased risk of suffering from a cyber-enabled economic warfare (CEEW) campaign — a series of cyberattacks intended to strike at critical infrastructure to undermine the economy, military capability, and American social cohesion.[2]

Even in the absence of an all-out conflict, Beijing has increasingly demonstrated its willingness to weaponize its hold over communications systems to advance its strategic objectives — tracking senior government officials, pursuing adversarial information operations to erode trust in institutions, and threatening the continuity of the economy. These efforts have been underwritten by changes in the nation's communications landscape, with China exploiting possible backdoors in popular home router systems, infiltrating telecoms networks, and subtly shaping mass opinion via control over social media platforms.[3]

Legacy systems, particularly radio and local television, play a key role in U.S. national security by offering redundancy to existing systems and providing a key avenue to mitigate CEEW campaigns. In the event of a crisis during which China chooses to target telecommunications infrastructure — as occurred during Salt Typhoon intrusions — legacy broadcast systems with

[1] Elisa Shearer, Katerina Eva Matsa, Michael Lipka, Kirsten Eddy and Naomi Forman-Katz, "Americans' Changing Relationship With Local News," *Pew Research Center*, May 7, 2024. (https://www.pewresearch.org/journalism/2024/05/07/americans-changing-relationship-with-local-news); Robin Buller, "These rural radio stations are a lifeline for their communities. Trump's cuts threaten their future," *The Guardian* (UK), August 14, 2025. (https://www.theguardian.com/us-news/2025/aug/14/rural-radio-stations-federal-funding-cuts)

[2] Samantha Ravich and Annie Fixler, "The Attack on America's Future: Cyber-enabled Economic Warfare," *Foundation for Defense of Democracies*, October 28, 2022. (https://www.fdd.org/analysis/2022/10/28/the-attack-on-americas-future-cyber-enabled-economic-warfare)

[3] 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)

national reach provide valuable backup capabilities that maintain critical lines of information sharing.[4]

This comment provides detail on the threat China poses to U.S. communications infrastructure and offers recommendations for the Federal Communications Commission (FCC) to safeguard national security within its quadrennial review process.

China Poses Significant Risks to U.S. Communications Infrastructure

China's recent behavior strongly suggests that Beijing views communications as key during a possible conflict with the United States. China has combined traditional espionage with sabotage capabilities throughout its cyberattacks on communications infrastructure within United States and among U.S. allies and partners. According to reports on Chinese cyber operations, China has likely collected data on every American while gaining entry into the critical infrastructure of nearly 80 countries worldwide.[5]

These campaigns also complement Beijing's broader efforts to target the United States — shaping not only the cyber-physical terrain of the nation's communication system, but also its content through adversarial information campaigns and influence over popular social media platforms. As audiences shift away from legacy media, Beijing has found new vulnerabilities to exploit through techniques ranging from algorithm manipulation that shapes perception of the Chinese Communist Party (CCP) to directly paying third-party influencers to "tell China's story well" (讲好中国故事).[6] This issue has gained salience within Washington, with the Supreme Court in Moody v. NetChoice noting that platforms controlled by foreign adversaries, increasingly positioned as substitutes for legacy broadcast systems, remain vulnerable to manipulation and interference.[7]

While aimed at Washington, previews of Beijing's strategy are currently on display in Taipei. In an October 2024 report to the parliament, the Taiwanese National Security Bureau (NSB) reported that government networks experienced 2.8 million intrusions daily, a 17 percent

---

[4] Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before the House Committee on Homeland Security*, March 5, 2025. (https://www.fdd.org/analysis/2025/03/05/countering-threats-posed-by-the-chinese-communist-party-to-u-s-national-security)

[5] Jack Burnham and Jiwon Ma, "Resilient Networks; Disruptions to Communications," *Foundation for Defense of Democracies*, October 2, 2025. (https://www.fdd.org/analysis/2025/10/02/resilient-networks-disruptions-to-communications)

[6] *TikTok Inc. v. Garland*, 604 U.S. 56 (SCOTUS 2025). (https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf)

[7] *Moody v. NetChoice, LLC*, 603 U.S. 707 (SCOTUS 2024). (https://supreme.justia.com/cases/federal/us/603/22-277); see also *TikTok Inc. v. Garland*, 604 U. S. 56 (SCOTUS 2025). (https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf)

increase from the year prior.[8] Many of these attacks targeted the communications sector alongside military, energy, and health care infrastructure — a strategy designed to produce cascading failures that inhibit economic activity and military mobility. These cyber-intrusions were followed by a dramatic rise in adversarial information campaigns targeting the island, aiming to spread public fear, discontent, and apathy to erode resilience and engineer the social conditions Beijing deems necessary to force capitulation.[9]

This pattern highlights both China's systemic efforts to manipulate the communications sector as part of its broader strategic objectives and America's current vulnerabilities. To safeguard U.S. national security, the FCC should recognize nationwide broadcast networks as key national security assets.

Technical Resilience of Legacy Broadcast Systems

Legacy broadcast systems have some built-in advantages that make them more resilient to disruption than internet-dependent communications platforms.

Traditional radio and television operate through one-way signal transmissions from towers to receivers, eliminating any return path that an adversary could exploit to compromise a transmitter. In contrast, streaming platforms rely on continuous two-way internet connectivity for authentication, content delivery, and system management — introducing multiple layers of infrastructure that can be targeted or disrupted.

Broadcast systems also run on dedicated spectrum, separate from the internet infrastructure that adversaries routinely probe and compromise. Intrusions such as Salt Typhoon hit telecommunication networks precisely because they route internet traffic.[10] By design, over-the-air transmission continues to function as long as a station's transmitter and antenna remain operational, even when other digital platforms experience outages.

Furthermore, current ownership rules maintain a geographically distributed network of locally owned broadcast stations rather than a handful of centralized facilities. While this distribution may carry higher operational costs, it significantly strengthens system resilience. An adversary seeking to meaningfully disrupt nationwide broadcast communications would need to

[8] "Government network hit by over 2.8 million cyberattacks a day: NSB," *Focus Taiwan*, October 13, 2025. (https://focustaiwan.tw/politics/202510130019)
[9] Ibid.
[10] Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before the House Committee on Homeland Security*, March 5, 2025. (https://www.fdd.org/analysis/2025/03/05/countering-threats-posed-by-the-chinese-communist-party-to-u-s-national-security)

compromise hundreds of independent facilities, not a few consolidated centers — ensuring that the loss of any single station does not undermine regional communications.

FCC's Key National Security Role in Regulating Media Ownership

The FCC's role in managing broadcast ownership standards positions the Commission to mitigate adversarial CEEW campaigns. Through oversight of local radio, broadcast television, and the Dual Network Rule, the FCC shapes the direction of legacy systems while enabling the prioritization of national security considerations.

In managing ownership regulations for legacy broadcast systems, the Commission shapes the resilience and operational reach of the nation's communications infrastructure. Alongside the FCC's Disaster Information Reporting System, legacy broadcast networks ensure economic continuity following disasters or attack by providing critical information and filling any gaps produced by a collapse of other communications systems. The FCC's oversight role also enables the Commission to strengthen the Integrated Public Alert and Warning System (IPAWS). Although the Department of Homeland Security (DHS) is responsible for managing IPAWS communications, the FCC's role in regulating broadcast infrastructure ensures that the Commission has a significant impact on the functionality of the country's main crisis communications system. During emergencies, IPAWS pushes alerts through broadcast stations that reach audiences when even internet and cellular networks are congested or compromised. This is also the case for the amateur radio network, a key node within the country's communications infrastructure. Amateur radio operators provide emergency communications when commercial systems fail, as demonstrated during numerous natural disasters.[11]

The Commission's quadrennial review process also directly shapes key national security priorities as part of fulfilling its overall policy goals of protecting competition, localism, and viewpoint diversity. While these goals may periodically conflict, each contributes to a vibrant and secure communications sector. By maintaining competition, localism, and viewpoint diversity within a national broadcast infrastructure, the United States benefits from redundancy through multiple market players, trusted news sources to counter adversarial cognitive warfare, and a broad ownership distribution that prevents concentrated foreign ownership and control.

[11] "Amateur Radio Emergency Service," *The National Association of Amateur Radio*, accessed December 3, 2025. (https://www.arrl.org/ares)

Balancing National Security With Economic Realities

Streaming services have not merely captured audience attention — they have fundamentally restructured advertising markets, eroding revenues while broadcasters continue to bear significant capital and operational costs. For many stations, consolidation has become the primary path to economic survival.

But the fact that consolidation makes economic sense does not negate its national security consequences. A highly centralized broadcast system may be more cost efficient, yet it also concentrates risk in ways that undermine communications resilience. Disruption of a few consolidated facilities can silence entire regions — an outcome that would be far less likely in a distributed ownership environment.

Economic pressures, however, should not be ignored. Protecting resilience does not mean freezing the market in place or forcing every station to operate at any cost. It means recognizing that preserving a minimally sufficient level of distributed, over-the-air capability is a national security function, not merely a market outcome. The Commission can approach this by ensuring that consolidation does not eliminate geographic redundancy, by coordinating with other federal partners on ways to support stations that serve essential public safety roles, and by monitoring where market contraction risks leaving communities dependent solely on internet-based communications.

The path forward is not about choosing national security over economics or vice versa. It is about recognizing that the national security value of distributed broadcast infrastructure does not show up on balance sheets yet remains integral to the country's ability to communicate during crises.

Recommendations for Prioritizing Nationwide Broadcast Infrastructure as a National Security Asset

In reviewing its media ownership regulations, the FCC should treat the maintenance of nationwide broadcast infrastructure as a national security priority by strengthening its quadrennial review process and rebalancing its public interest motivation in the regulation of local radio and television networks.

- **The FCC should integrate "national security" as an explicit policy goal for future quadrennial reviews.** The Commission should establish "national security" as a parallel goal to its existing mandates to consider localism, competition, and viewpoint diversity in reviewing ownership rules. This will codify the importance of national broadcast

systems to America's resilience and defense posture while providing a foundation for future policymaking aimed at protecting against adversarial CEEW campaigns. In practice, this means requiring that proposed rule changes undergo analysis of their impact on communications resilience during crisis scenarios, including evaluation of whether changes would create single points of failure or reduce redundancy.

- **The FCC should consider nationwide broadcast infrastructure to be a national security asset.** While streaming and other forms of broadcast media have become increasingly popular, maintaining legacy nationwide broadcast systems remains critical due to their form and function. Local radio and television possess stronger protections against cyber interference compared to internet-based systems while maintaining broad geographic reach. The FCC's focus on localism and competition naturally impedes foreign adversaries' efforts to manipulate information while offering a trusted counterweight to adversarial cognitive warfare. This designation should be accompanied by periodic reporting on the health and geographic distribution of broadcast infrastructure to enable informed policymaking.

- **The FCC should explicitly coordinate with DHS in providing input on local media ownership rules.** While the FCC maintains oversight of local media ownership regulations, the Federal Emergency Management Agency under DHS has a key role in maintaining disaster communications systems such as IPAWS. The Commission should establish a formal interagency process requiring DHS/FEMA input on proposed ownership requirements and rule changes, with specific focus on impacts to emergency communications capability. This coordination should include regular exercises testing the broadcast network's ability to function as a backup during telecommunications infrastructure failures.

- **The Commission's Local Radio Ownership Rule remains in the public interest and strengthened.** Rather than relaxing ownership rules in response to economic pressure, the FCC should maintain current restrictions while working with Congress and other agencies to explore support mechanisms that preserve the national security benefits of distributed ownership. This may include prioritizing locally owned stations for participation in emergency communications programs or creating incentives for ownership structures that maintain local operations.

- **The Commission should treat broadcast radio as a discrete market from audio streaming for ownership regulation purposes.** While audio streaming services, such as podcasts or internet radio, have become popular, they cannot effectively replace legacy systems due to their vulnerability to adversarial cyberattacks and the medium's inherent incompatibility with rapid crisis response communication. Moreover, these platforms do

not comply with FCC ownership requirements, creating openings for foreign adversaries to use them for information operations against the United States and its allies and partners. For purposes of calculating market concentration and evaluating ownership applications, the FCC should analyze broadcast radio separately from internet-based audio services, recognizing their fundamentally different technical characteristics and national security implications. This approach acknowledges that while these platforms compete commercially, they are not equivalent from a resilience perspective.

- **The Commission's Local Television Ownership Rule remains in the public interest.** The current rule adequately serves the Commission's public interest goals of competition, localism, and viewpoint diversity, particularly given licensees' obligations to serve local communities in exchange for access to public airwaves. While these stations have lost audience share to streaming services, they maintain high levels of public trust, making them critical assets to counter adversarial cognitive warfare campaigns. The FCC should maintain current ownership restrictions for television while monitoring whether consolidation trends threaten to create coverage gaps in specific geographic regions.

- **The FCC should assess and report on communications resilience metrics.** To enable informed policymaking, the Commission should establish and regularly report on metrics that measure the national security value of broadcast infrastructure. These measures might include the percentage of the U.S. population with access to locally owned broadcast radio and television independent of internet infrastructure, the geographic distribution of broadcast facilities, diversity of ownership, and redundancy measures. These metrics should inform quadrennial reviews and provide transparency to Congress and the public regarding trends in communications resilience.

Conclusion

The FCC should consider the health and maintenance of nationwide broadcast networks to be a national security priority throughout its quadrennial review of local media ownership rules. Thank you for considering our comments. We look forward to seeing how these national security considerations are incorporated into the review process.