Federal Communications Commission

Advancing IP Interconnection

47 CFR Part 51
[WC Docket Nos. 25-304, 25-208, 17-97; FCC 25-73; FR ID 319327]

AUTHORS

Jack Burnham
Senior Research Analyst, FDD's China Program

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

Craig Singleton
Senior Director and Senior Fellow, FDD's China Program

Washington, DC
December 17, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

China's unprecedented breaches of America's telecommunications network highlight both Beijing's growing aggression in cyberspace and severe vulnerabilities within the country's critical infrastructure. Chinese hackers, dubbed "Salt Typhoon," collected intelligence on nearly every American, breached military communications systems, and were allegedly able to track senior U.S. government officials, potentially enabling Beijing to pursue a surprise decapitation strike in the event of a crisis. This campaign follows China's other cyberspace attacks, including "Volt Typhoon," which penetrated critical infrastructure necessary for military mobility; "Flax Typhoon," which targeted communications infrastructure connecting the United States and Taiwan; and other attacks against U.S. government agencies.

Amid these attacks, the United States still maintains some aging legacy telecommunications infrastructure that cannot easily be modernized or secured, leaving a persistent vulnerability. Though the industry is slowly phasing out these interconnect systems, such as time-division multiplexing (TDM), they are still prevalent within rural areas, between regional and national carriers, and within critical sectors, such as airspace control systems. Outdated FCC regulations are encouraging their presence and forcing carriers to expend limited resources to meet aging requirements rather than investing in modernization. Moreover, the transition to newer systems, such as routing voice communications using an internet protocol system (IP), remains in flux due to intra-carrier negotiations over security regulations and a lack of an overarching cybersecurity plan to replace previous efforts undertaken in the immediate aftermath of Salt Typhoon's operation.

As such, the Federal Communications Commission (FCC) should use its oversight and regulatory authorities to encourage carriers to adopt an all-IP interconnect system and comply with more stringent cybersecurity practices to safeguard U.S. national security.

Chinese Hacking Group Known as 'Salt Typhoon' Targeted U.S. Telecommunications

China has engaged in operational preparation of the battlefield — identifying vulnerabilities within existing telecommunications networks and establishing permanent access points that can be used to conduct espionage or sabotage operations in the event of a crisis with the United States. Beginning at least as early as 2021, Chinese state-affiliated hackers known collectively as "Salt Typhoon" began targeting the telecommunications sector of the United States and its allies and partners.

This campaign, which far exceeded previous efforts, collected intelligence, established a presence on networks used for intelligence collection, and potentially tracked the movements of high-level U.S. officials, raising the possibility of a decapitation strike in the event of an all-out

conflict.[1] The attack also hit at least one Army National Guard unit, including mapping base infrastructure and exfiltrating service members' information, highlighting Beijing's efforts to target U.S. military capabilities far outside of the Indo-Pacific theater.[2]

Combined, these campaigns highlight that China perceives U.S. telecommunications networks as a key center of gravity in a possible conflict, both due to their role in ensuring continuity of the economy and upholding military mobility, and their overall importance to societal stability.[3]

The success of Salt Typhoon was partly a reflection of poor cybersecurity standards within a complex and evolving industry. According to publicly released U.S. and allied intelligence, the attack did not rely on "zero-day" vulnerabilities — unknown flaws that are inadvertently embedded within software or hardware products — but rather leveraged poorly connected systems and known but unpatched faults in current software to penetrate telecommunication firms' internal infrastructure.[4] This cascading series of failures, beginning with vulnerabilities embedded within edge devices, likely allowed Chinese hackers to move laterally across networks and install exfiltration points while evading detection from both the private sector and government authorities.

The FCC Should Support Modernizing America's Telecommunications Infrastructure

These risks have emerged just as the United States remains on the cusp of phasing out legacy systems, such as TDM, from most of its telecommunications infrastructure and switching to an all Voice over IP (VOIP) system. This move, if properly overseen by the Commission, will likely enhance U.S. national security by producing a more reliable, secure system even as the process may present challenges for certain sectors and regions.

As with other aging infrastructure, systems such as TDM present a series of security risks due to their growing obsolescence. Given their aging code bases, inability to execute rapid software

---

[1] 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); 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); Adam Goldman, "'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American," *The New York Times*, September 4, 2025. (https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html)

[2] David DiMolfetta, "Salt Typhoon hacks into National Guard systems a 'serious escalation', experts warn," *Nextgov/FCW*, July 16, 2025. (https://www.nextgov.com/cybersecurity/2025/07/salt-typhoon-hacks-national-guard-systems-serious-escalation-experts-warn/406765)

[3] 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)

[4] "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," *Cyber and Infrastructure Security Agency*, September 3, 2025. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a)

patches, and limited capacity to adopt aftermarket security updates, TDM pose a small, but persistent vulnerability within the country's telecommunications infrastructure. These issues will only escalate as more carriers and customers switch to alternative systems, further dampening the demand necessary to sustain the companies that can maintain aging systems.

While not directly under the Commission's purview, these vulnerabilities also have a direct impact on other critical infrastructure operators vital to military mobility, namely the Federal Aviation Administration (FAA) and some railroad systems. While the FAA has sought to modernize aspects of its air traffic control systems, many of the agency's radar stations used to monitor national and regional air routes rely on legacy communications architecture, including TDM, to continue operations.[5] Similarly, railroads continue to rely on TDM for some communication and signaling systems, partially due to its simplicity and a lack of sustained investment in more secure alternatives.[6] Given the reliance of the U.S. military on these systems to manage the flow of forces from interior bases to disembarkation points and into theater, these issues threaten Washington's capabilities to rapidly respond to a global military crisis.[7]

As such, the Commission's efforts to accelerate a transition to an all-IP system can enhance U.S. national security directly by strengthening telecommunications infrastructure as well as indirectly by spurring broader modernization efforts in other sectors. While all-IP systems unfortunately also remain vulnerable to cyberattacks, as demonstrated by Salt Typhoon, they are easier to monitor, uphold stronger encryption standards, remain more amendable to modernization, and provide greater regional coverage.

Recommendations

Using its oversight of the country's telecommunications sector, the FCC should encourage carriers to migrate to an all-IP system while providing strong, scalable cybersecurity standards to protect carriers and critical infrastructure. These reforms will protect the United States from adversarial espionage and sabotage while offering a signal to other executive agencies and departments to prioritize modernization efforts.

- **The FCC should use its regulatory authority to encourage a transition to an all-IP interconnect system.** This switch will bolster the overall security of the telecommunications industry while allowing for greater modernization to confront emerging risks stemming from adversarial behavior. The FCC should exercise forbearance on enforcing compliance with Section 251(c) of the Telecommunications Act

[5] U.S. Federal Aviation Administration, "TDM-to-IP Migration," October 27, 2015. (https://www.faa.gov/sites/faa.gov/files/air_traffic/technology/cinp/fens/tdm-to-ip_migration_2015-10-27.pdf)
[6] "Time Division Multiplexer for railway applications," *Unipart Rail*, accessed December 9, 2025. (https://www.unipartrail.com/wp-content/uploads/2020/04/telecode_tdm-compressed.pdf)
[7] 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)

of 1996, allowing carriers to invest in building out more secure systems rather than having to expend additional resources maintaining legacy equipment.

- **The FCC should encourage, to the extent possible, critical infrastructure providers to transition to an all-IP system.** While the FCC has limited oversight over other agencies, such as the FAA, the Commission should publicize the security enhancements offered by an all-IP system during its public meetings and proceedings to encourage other executive agencies and departments to consider modernizing their communications infrastructure.

- **The FCC should develop robust cybersecurity standards for carriers to secure an all-IP system.** While the Commission removed certain cybersecurity requirements imposed in the immediate aftermath of Salt Typhoon's emergence, the FCC should develop and enforce robust security standards for the communications sector. These standards should guide licensing decisions and be incorporated into future proceedings related to modernizing the industry.

- **The FCC should provide support for intra-carrier negotiations over cybersecurity protocols.** As carriers transition to an all-IP system, the Commission should encourage the industry to adopt a robust security framework for communications passed between carriers. While these communications are routinely secured using a variety of methods, the FCC can encourage carriers to adopt a single encryption standard to ease compliance burdens and prevent vulnerabilities from developing across transit points.

Conclusion

The FCC's push to modernize America's telecommunications sector by encouraging the adoption of an all-IP system for voice communications is a critical step forward in countering Chinese adversarial behavior and improving U.S. national security. Thank you for considering our comments, and we look forward to seeing how our input is incorporated into the final rule.