Federal Communications Commission

Resilient Networks; Disruptions to Communications

Docket No 47 CFR Part 4
[PS Docket Nos. 21-346, 15-80, ET Docket No. 04-35; FCC 25-45; FR ID 310513]

AUTHORS

Jack Burnham
Research Analyst, FDD's China Program

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

Washington, DC
October 2, 2025

Introduction

China poses an unprecedented cyber threat to the United States, having evolved from a clear follower into a near-peer adversary capable of executing sophisticated operations against broad swaths of the U.S. telecommunications network. These and other cyber campaigns threaten the continuity of the economy, undermine public trust, and jeopardize military mobility.

Beijing's "Salt Typhoon" campaign penetrated communications infrastructure in nearly 80 countries. The "Volt Typhoon" campaign prepositioned disruptive capabilities across U.S. critical infrastructure.[1] Beyond infiltrating networks to conduct espionage and prepare the battlefield, China has rehearsed the use of malign information operations to amplify these effects, eroding public confidence in government and creating societal instability that delays response efforts.[2]

These developments require the Federal Communications Commission (FCC) to not only regulate but also partner with industry and state authorities to strengthen resilience against cyberattacks. The FCC has already made progress in streamlining certain reporting requirements; building on that progress, it should now focus on modernizing the Disaster Information Reporting System (DIRS). DIRS provides critical situational awareness across communications service providers, agencies, and the public during both natural and manmade disasters. The FCC should modernize DIRS in ways that both reduce unnecessary burdens and enhance national preparedness.

Congress, through Section 1 of the Communications Act, explicitly directs the FCC to "make available … communication service with adequate facilities … for the purpose of promoting safety of life and property."[3] The FCC can operationalize this mandate by requiring service outage reporting across key services. Modernizing DIRS is, therefore, not only good policy but a statutory responsibility.

China's Shift Toward Strategic Cyber Sabotage

China's strategic objectives have shifted from advancing its domestic development to building deep-strike offensive cyber capabilities against an adversary. Whereas earlier operations were largely limited to espionage and data theft; today, Beijing demonstrates both the intent and the

---

[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); 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] Bradley Bowman, "Cognitive Combat: China, Russia, and Iran's Information War Against Americans," *Foundation for Defense of Democracies*, June 28, 2024. (https://www.fdd.org/analysis/monographs/2024/06/28/cognitive-combat/); Jaime Ocon and Jonathan Walberg, "China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities," *Global Taiwan Institute*, June 4, 2025. (https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities)

[3] Purposes of chapter; Federal Communications Commission created, 47 U.S.C. §151. (https://www.law.cornell.edu/uscode/text/47/151)

means to carry out more sophisticated strikes and degrade the safe and reliable operation of U.S. critical infrastructure in ways that could produce economic and military aftershocks.[4]

The "Volt Typhoon" campaign marked this transition. Chinese hackers penetrated U.S. critical infrastructure essential to both economic stability and military mobility, increasing the likelihood of sabotage in the event of a military crisis in the Indo-Pacific.[5] The Salt Typhoon campaign deepened this threat, embedding Chinese actors within U.S. telecommunications networks where they could monitor the communications of senior U.S. government officials and infiltrate military systems.[6]

Moreover, China is also refining the practice of pairing cyberattacks with influence operations that erode national morale and sow distrust. In Taiwan, Beijing tested this playbook by using commercial vessels to sever undersea cables while simultaneously launching disinformation campaigns that falsely blamed Taipei, an approach it could readily replicate against the United States.[7]

The consequences of such an attack would be profound and systemic: disrupted communications would paralyze economic activity,[8] complicate recovery efforts, and delay military mobilization. Adversarial information operations would compound the issue, causing public panic, economic

---

[4] Jack Burnham and Jiwon Ma, "The Pentagon Has Given China Access to Its Systems for Over a Decade," *Foundation for Defense of Democracies*, July 16, 2025. (https://www.fdd.org/analysis/2025/07/16/the-pentagon-has-given-china-access-to-its-systems-for-over-a-decade); Bradley Bowman, Michael Minihan, Mark Montgomery, and Annie Fixler, "Persistent Access, Persistent Threat: Ensuring Military Mobility Against Malicious Cyber Actors," *Panel Discussion hosted by the Foundation for Defense of Democracies*, April 17, 2025. (https://www.fdd.org/events/2025/04/17/persistent-access-persistent-threat-ensuring-military-mobility-against-malicious-cyber-actors)

[5] Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before 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); Erica Lonergan and Mark Montgomery, "Building the Future U.S. Cyber Force," *Foundation for Defense of Democracies*, September 9, 2025. (https://www.fdd.org/analysis/2025/09/09/building-the-future-us-cyber-force); 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)

[6] 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); Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before 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)

[7] Jaime Ocon and Jonathan Walberg, "China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities," *Global Taiwan Institute*, June 4, 2025. (https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities); Mark Montgomery, Johanna Yang, Craig Singleton, and Jack Burnham, "10 Takeaways From Simulated Attacks on Taiwan's Energy Sector," *Foundation for Defense of Democracies*, September 4, 2025. (https://www.fdd.org/analysis/2025/09/04/10-takeaways-from-simulated-attacks-on-taiwans-energy-sector)

[8] Mark Harvey and Mark Montgomery, "After the Attack: A Playbook for Continuity of the Economy Planning and Implementation," *Foundation for Defense of Democracies*, September 13, 2025. (https://www.fdd.org/wp-content/uploads/2023/09/fdd-memo-cote.pdf); Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before 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)

disorder, and the erosion of public confidence in government. The ability to degrade the safe operation of ports, airports, and rail networks directly threatens U.S. deterrence in the Indo-Pacific and beyond.[9] In short, China is developing the means not just to spy on American systems, but to strategically hold them at risk in ways that magnify crisis instability.

DIRS's Role in Countering Adversarial Cyber Operations

A large-scale cyberattack would in many respects largely resemble the cascading effects of a natural disaster — communications failures, denial of service, and infrastructure degradation.[10] Unlike natural hazards, however, cyber disruptions would almost certainly be compounded by adversarial information campaigns designed to inflame panic and undermine confidence in authorities.[11]

The DIRS, created after the devastation caused by Hurricane Katrina in 2005, serves as a centralized process for providers to report service status and request assistance. When DIRS is activated, the FCC requests daily situation reports from participating providers, such as cable and wireless communication companies, on the operational status of their networks, including outages, fuel availability, and restoration progress. These reports are then aggregated into near-real-time situational updates for federal, state, and local officials, enabling them to prioritize resources such as fuel deliveries or repair crews. Providers are expected to submit reports even if their systems remain fully operational, ensuring that officials can distinguish between unaffected networks and non-reporting entities. They must also file a final closure report within 24 hours of deactivation — the point at which the FCC ends emergency reporting once conditions have stabilized — ensuring accountability and providing a definitive record for planning repairs and analyzing outages. The FCC underscored the value of outage reporting, noting that "even limited information disclosure … can spur industry-wide" collaboration and can make networks more reliable, among other improvements.[12] Similarly, the Government Accountability Office has recommended improving the FCC's collection and sharing of outage information in order to better coordinate with the Department of Homeland Security and first responders.[13]

DIRS's integration across providers, state and local governments, and federal agencies makes it the logical foundation for a common operating picture. Natural disasters in the United States with prolonged outages, like Hurricane Maria in 2017, hinder emergency communications. For instance, 96 percent of telecommunications facilities were out of service in Puerto Rico after the

---

[9] Annie Fixler, Mark Montgomery, 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)

[10] Anne Neuberger, "China Is Winning the Cyberwar," *Foreign Affairs*, August 13, 2025. (https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence); Chris Nolan and Annie Fixler, "The Economic Costs of Cyber Risk," *Foundation for Defense of Democracies*, June 28, 2021. (https://www.fdd.org/analysis/2021/06/28/the-economic-costs-of-cyber-risk)

[11] Mark Montgomery, Johanna Yang, Craig Singleton, and Jack Burnham, "10 Takeaways From Simulated Attacks on Taiwan's Energy Sector," *Foundation for Defense of Democracies*, September 4, 2025. (https://www.fdd.org/analysis/2025/09/04/10-takeaways-from-simulated-attacks-on-taiwans-energy-sector)

[12] U.S. Government Accountability Office, "FCC Assisted in Hurricane Maria Network Restoration, but a Clarified Disaster Response Role and Enhanced Communication Are Needed," April 29, 2021, page 12. (https://www.gao.gov/assets/gao-21-297.pdf)

[13] Ibid.

storm.[14] In 2023, during the Maui, Hawaii, wildfires, gaps in reporting delayed situational awareness and contributed to confusion over the scope of outages, slowing the coordination of emergency alerts and resource deployment.[15] These disasters underscore the dangers of fragmented information — when officials lack timely and accurate data, emergency responders cannot effectively prioritize resources, leaving the public exposed to confusion, rumors, and disinformation. The same lessons would apply to cyber incidents, where simultaneous technical disruptions and disinformation campaigns could paralyze decision-making and give adversaries openings to shape public perception. A trusted and centralized reporting system like DIRS is critical to enable coordination, reinforce public trust, and deny adversaries the ability to manipulate the information environment.

Recommendations

To enhance the resilience of the communications sector, the FCC should improve its data collection practices by expanding mandatory reporting requirements and improving access to collected data. Combined, these efforts will allow DIRS to generate a more accurate and comprehensive common operating picture during crises, thereby improving coordination among providers, state and federal responders, and the public. At the same time, greater transparency would blunt the effectiveness of adversarial influence campaigns that seek to exploit uncertainty in the wake of major incidents.

- **Maintain mandatory reporting for cable, wireline, wireless, and interconnected VoIP providers**. Chinese operators have demonstrated their ability to penetrate deeply into telecommunications networks. While these operations have focused thus far on espionage, China may be able to use this same access to disrupt communication systems. By requiring consistent reporting across these networks, the FCC can ensure that DIRS captures the baseline operational status of the systems most essential to national resilience. This rule is not about imposing additional burdens; this requirement leverages data that providers already collect, ensuring it is used to its fullest value in strengthening national resilience.

- **Expand mandatory reporting to broadband, satellite, and other communications service providers**. China's campaigns have increasingly focused on targeting broadband and satellite service providers, reflecting the growing importance of these systems to both the economy and military operations. Broadband networks underpin critical services from telemedicine to logistics, while satellite connectivity is indispensable for global coordination in both civilian and defense contexts. Incorporating these providers into mandatory DIRS reporting would give federal, state, and local responders a more complete view of America's operational baseline and enable more precise recovery

[14] U.S. Government Accountability Office, "FCC Assisted in Hurricane Maria Network Restoration, but a Clarified Disaster Response Role and Enhanced Communication Are Needed," April 29, 2021, page 2. (https://www.gao.gov/assets/gao-21-297.pdf)

[15] Maui Emergency Management Agency, "After-Action Report, Maui Wildfires 2023," January 24, 2025, page 9. (https://www.mauicounty.gov/DocumentCenter/View/151355/MEMA-2023-Wildfire-After-Action-Report); Maui Police Department, "Maui Wildfires of August 8, 2023 Maui Police Department Preliminary After-Action Report," August 1, 2025, page 58. (https://www.mauipolice.com/_files/ugd/fefc36_d7b72f6a0ca9458d93391093da02fe1e.pdf)

planning. A phased expansion would ensure no critical segment of the communications ecosystem is left unmonitored during a crisis, while giving providers time to integrate reporting smoothly.

- **Require all reporters to submit streamlined closure reports within 24 hours of event deactivation**. While recovery timelines are inherently variable, a standardized final submission offers value for future disaster planning and recovery. It provides state and local authorities with a definitive snapshot of restoration, informs after-action assessments, and helps inoculate the public against adversarial disinformation campaigns. To reduce burdens on providers, the FCC could adopt a simplified "one-click closure" mechanism, balancing efficiency with accountability.

- **Simplify secure access to DIRS for authorized users**. DIRS is only as effective as its capacity to deliver timely insights to the number of agencies and organizations able to use it in real time. At present, participation is low among emergency management agencies due to cumbersome authorization and training requirements. Streamlining access lowers barriers for responders and increases uptake. For instance, the FCC can streamline processes by eliminating duplicative recertifications while ensuring strong cybersecurity protections. Expanding access would ensure that DIRS fulfills its purpose as a national resource rather than a narrowly used tool.

- **Adopt a tiered transparency model for greater public access to DIRS reporting information**. The public must have confidence in the resilience of the U.S. communications systems, particularly during a crisis. By releasing aggregated outage and restoration data with secure measures to keep provider-specific information protected, the FCC can reinforce trust. At the same time, greater visibility into performance creates a market incentive: if customers see that one provider consistently restores service faster or remains operational during disasters, they are more likely to switch to that provider, driving competition on the basis of resilience. The FCC has already piloted limited public release of DIRS data during hurricanes.[16] Done carefully, institutionalizing this model of balancing transparency and security could transform DIRS from a compliance mechanism into a strategic asset that prevents adversaries from filling an information vacuum with false narratives.

Conclusion

China's recent cyber campaigns illustrate how nation-state adversaries intend to exploit communications networks as both a technical and psychological battlespace. The FCC is uniquely positioned to mitigate these risks. The FCC has both the statutory authority and the practical precedent to act decisively. By modernizing DIRS now, the FCC can close known gaps and ensure the nation's communications networks are resilient not only to natural disasters but also to cyberattacks.

We look forward to seeing how our feedback is used to inform the FCC's future efforts.

[16] U.S. Federal Communications Commission, "Communications Status Report for Areas Impacted by Hurricane Helene," October 8, 2024, page 1. (https://docs.fcc.gov/public/attachments/DOC-406312A1.pdf)