BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

MEMORANDUM

To: Members, Energy and Commerce Committee
From: Majority Staff
Re: Communications and Technology Subcommittee Hearing

I. INTRODUCTION

On Wednesday, April 30, 2025, at 10:00am, the Subcommittee on Communications and Technology will hold a hearing in 2322 Rayburn House Office Building entitled, "Global Networks at Risk: Securing the Future of Communications Infrastructure." The following witnesses are expected to testify:

II. WITNESSES

- Tom Stroup, President, Satellite Industry Association
- David Stehlin, Chief Executive Officer, Telecommunications Industry Association
- Jamil N. Jaffer, Founder and Executive Director, National Security Institute
- Laura Galante, former Intelligence Community Cyber Executive and Director, Cyber Threat Intelligence Integration Center, Office of the Director of National Intelligence

III. BACKGROUND

The United States has always been at the forefront of innovation, and over the last century has led the development of digital devices and services that Americans rely on in daily life. Americans learn, work, receive health care services, and stay in touch with friends and loved ones online. As our society becomes more connected, it is even more critical that the equipment we utilize is secure. With the known vulnerabilities in many technologies produced by entities with ties to foreign adversaries, including the Chinese Communist Party (CCP) specifically, we must take steps to reduce the widespread availability of this equipment that poses a national security threat in the United States.[1]

---

[1] *The China Threat,* The Federal Bureau of Investigation, https://www.fbi.gov/investigate/counterintelligence/the-china-threat (last visited Apr. 11, 2025).

In recent decades, the CCP has taken aggressive steps to position China to overtake the United States and its allies as the world's preeminent economic power.[2] The CCP invested heavily into a range of industries domestically to become less dependent on the United States and its allies for China's critical infrastructure.[3] In the case of communications infrastructure, CCP-backed companies developed unsecure telecommunications equipment and exported it around the world in order to assist in its espionage activities.[4]

On March 13, 2025, Federal Communications Commission (FCC) Chairman Brendan Carr announced that he will establish a new Council for National Security within the FCC. The Council seeks to:

> (1) Reduce the American technology and telecommunications sectors' trade and supply chain dependencies on foreign adversaries; (2) Mitigate America's vulnerabilities to cyberattacks, espionage, and surveillance by foreign adversaries; and (3) Ensure the U.S. wins the strategic competition with China over critical technologies, such as 5G and 6G, AI, satellites and space, quantum computing, robotics and autonomous systems, and the Internet of Things.[5]

IV. SELECTED ISSUES

Chinese Communist Party Influence

American officials note the "increasingly authoritarian nature of the CCP, the fading line between independent business and the state, and new laws that will give Beijing the power to look into, or maybe even take over, networks that companies like Huawei have helped build and maintain."[6] Specifically, they point to China's 2017 National Intelligence Law, which "requires Chinese companies to support, provide assistance and cooperate in China's national intelligence work, wherever they operate," which could implicate equipment they sell in the United States.[7] Further, the opaque ownership structures of Chinese companies raise even more questions

---

[2] Matthew Reynolds, *Standing United Against the People's Republic of China's Economic Aggression and Predatory Practices,* CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (May 18, 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/ts230517_Reynolds_Economic_Aggression.pdf?VersionId=xNi8qfzihhppiwXpriMd5uRUrzdpXFH2.

[3] Anshu Siripuranu and Noah Berman, *The Contentious U.S.-China Relationship,* COUNCIL ON FOREIGN RELATIONS (Sept. 26, 2023), https://www.cfr.org/backgrounder/contentious-us-china-trade-relationship.

[4] *A Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, Permanent Select Committee on Intelligenc*e, U.S. House of Representatives 112th (Oct. 8, 2012), https://intelligence house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[5] *Chairman Carr Establishes New Council on National Security Within Agency*, Office of Chairman Brendan Carr, Federal Communications Commission (March 13, 2025), https://docs fcc.gov/public/attachments/DOC-410155A1.pdf

[6] David E. Sanger et al., *In 5G Race With China, U.S. Pushes Allies to Fight Huawei*, N.Y. TIMES (Jan. 26, 2019), https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology html.

[7] *Id.*

related to how much influence the Chinese government can assert over them, leading to uncertainty about the national security threats posed by Chinese technology.[8]

Supply Chain Security

On March 12, 2020, President Donald J. Trump signed the Secure and Trusted Communications Networks Act (STCNA) of 2019 into law.[9] The law prohibits a Universal Service Fund (USF) recipient from purchasing, obtaining, or maintaining any equipment or services from companies posing a national security threat, and requires the FCC to publish a list of "covered communications equipment or services" within one year that pose such a threat, which includes CCP-affiliated companies, including Huawei and ZTE.[10] The law also established a program to reimburse eligible communications providers for replacing covered communications equipment or services. Through the Consolidated Appropriations Act, 2021, Congress provided $1.9 billion to the FCC for the reimbursement program.[11] Demand for this program exceeded the initial estimate, resulting in a shortfall of $3.08 billion.[12] In the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Congress provided the FCC with the authority to borrow $3.08 billion from the Department of Treasury to fully fund the program shortfall, to be repaid with proceeds from a spectrum auction.[13]

On November 11, 2021, President Joseph R. Biden signed the Secure Equipment Act into law. This law requires the FCC to adopt rules updating its equipment authorization procedures to no longer consider any applications for equipment that is on the list of covered communications equipment and services published by the FCC pursuant to section 2(a) of STCNA. The FCC adopted those rules on November 25, 2022.[14]

Cybersecurity

Adversarial nations like the People's Republic of China (PRC), the Russian Federation, Iran, and North Korea engage in malicious cyber activity targeted against U.S. data and critical infrastructure.[15] Hackers exploit untrusted vendor equipment, as well as poor cyber hygiene and unsecure edge devices, among other vulnerabilities to gain access to our communications networks and sensitive data. According to the Cybersecurity and Infrastructure Security Agency

---

[8] Raymond Zhong, *Who Owns Huawei? The Company Tried to Explain. It Got Complicated.,* N.Y. TIMES (Apr. 25, 2019), https://www nytimes.com/2019/04/25/technology/who-owns-huawei html.
[9] *Supra* note 4.
[10] *List of Equipment and Services Covered by Section 2 of The Secure Networks Act,* The Federal Communications Commission, https://www fcc.gov/supplychain/coveredlist (last visited Apr. 11, 2025).
[11] Consolidated Appropriations Act, 2021 § 906(2).
[12] Letter from Jessica Rosenworcel, Chair, FCC, to the Hon. Maria Cantwell et al. (July 15, 2022), https://docs.fcc.gov/public/attachments/DOC-385335A1.pdf.
[13] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, div. E, tit. LIV § 5401 et seq. (2024).
[14] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232 et al., Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84 (rel. Nov. 25, 2022), https://docs fcc.gov/public/attachments/FCC-22-84A1.pdf.
[15] Nation-State Cyber Actors, CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.

(CISA), cyber actors sponsored by the PRC specifically "[seek] to pre-position themselves on information technology (IT) networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States."[16]

In the fall of 2024, reports emerged that hackers infiltrated U.S. telecommunications companies' networks in one of the largest intelligence compromises in U.S. history.[17] The Federal Bureau of Investigation (FBI) and CISA later confirmed these reports and that the threat was tied to the CCP.[18] This breach, known as Salt Typhoon, impacted at least 9 communications providers and enabled the hackers to "geolocate millions of individuals and record phone calls at will," impacting senior U.S. officials, including then President-elect Trump and Vice President-elect Vance.[19]

Undersea Cables

Undersea cables are responsible for carrying data traffic across oceans. There are more than 600 active and planned submarine cable systems that keep the world connected.[20] These cables are vulnerable to damage by the elements and unintentional acts, such as anchors dragging along the seafloor. Unfortunately, damage to these cables can result in service disruptions and can be costly and time-consuming to repair. For instance, in January, a cable serving northwest Alaska was severed, disrupting internet service for 20,000 Alaskans. Due to conditions where the cable is laid, including the presence of sea ice, the cable is not expected to be repaired for many months.[21]

Undersea cables have also been intentionally sabotaged. Taiwan depends on fourteen submarine cables to keep it connected to the global internet.[22] Multiple incidents involving Chinese-flagged vessels cutting cables connected to Taiwan over recent years have been documented.[23] In response, Taiwan has continued efforts to secure its connectivity by adding

---

[16] People's Republic of China Cyber Threat, CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china.
[17] Kevin Collier, *Telecoms haven't notified most victims of Chinese phone data hacking campaign*, sources say, NBC NEWS (Dec. 12, 2024), https://www nbcnews.com/tech/security/phone-hack-data-chinese-salt-typhoon-metadata-fbi-security-encrypt-rcna183233.
[18] Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications (Oct. 25, 2024), https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-prc-activity-targeting-telecommunications.
[19] Rosie Perper, *Chinese hackers used broad telco access to geolocate millions of Americans and record phone calls*, POLITICO (Dec. 27, 2024), https://www.politico.com/news/2024/12/27/chinese-hackers-telco-access-00196082.
[20] *Submarine Cable Frequently Asked Question*, TELEGEOGRAPHY (Apr. 24, 2025), https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.
[21] Zachariah Hughes, *Beaufort Sea ice cuts fiber-optic cable, limiting internet for about 20,000 residents of Northwest Alaska through summer*, ANCHORAGE DAILY NEWS (Feb. 4, 2025), https://www.adn.com/alaska-news/rural-alaska/2025/02/04/beaufort-sea-ice-snips-fiber-optic-cable-limiting-internet-for-some-20000-in-northwest-alaska-until-after-summer/.
[22] Chung Li-hua and Jonathan Chin, *Taiwan to add subsea Internet Cables,* TAIPEI TIMES (Apr. 16, 2023), https://www.taipeitimes.com/News/front/archives/2023/04/16/2003798023.
[23] Wayne Chang, *Taiwan detains Chinese-crewed ship suspected of cutting undersea cable,* CNN (Feb. 26, 2025), https://www.cnn.com/2025/02/25/asia/taiwan-detains-ship-undersea-cable-intl-hnk/index.html.

new cables and looking at alternative technologies to provide emergency backup and network redundancy, including satellite solutions.[24]

Satellites

Communications services provided by satellite operators are an important component of the marketplace. Satellite operators provide broadband service to homes and businesses as well as mission critical services like highly reliable voice, video, data, and observation capabilities to critical infrastructure companies and the federal government.[25] The FCC is responsible for authorizing the use of electromagnetic spectrum (spectrum) in the United States, and therefore, plays an important role in advancing the availability of satellite-provided communications services.[26]

In general, satellite providers operate at different altitudes above Earth. Satellites operate in either a geostationary satellite orbit (GSO) or in a non-geostationary satellite orbit (NGSO). GSO satellite systems rotate around the Earth at the same speed that the Earth rotates. They operate approximately 22,300 miles above earth. NGSO systems, on the other hand, can operate at varying altitudes, and many current and proposed systems operate closer to Earth in Low Earth Orbit (LEO). NGSO systems can also operate in Medium Earth Orbit (MEO) or High Earth Orbit (HEO).

Satellite communications services are an inherently global enterprise. Satellite operators provide services in markets around the world, so international harmonization of satellite spectrum use is critical. The International Telecommunications Union (ITU)—a division of the United Nations—manages a global table of spectrum allocations. This table represents treaty-level agreements where countries agree to define uses for certain spectrum frequencies in different regions across the world. National regulators, like the FCC in the United States, must therefore update their regulations in accordance with the wireless regulations of the ITU. Additionally, the ITU plays an important role in managing orbital slots for GSO and NGSO systems. The location of satellites in orbit are an important component of determining the spectrum usage of each satellite and therefore are considered in deliberations at the ITU and the FCC when licensing satellite communications systems.

Satellite systems can be expensive and difficult to repair. Some of these systems do not have many redundancies built into their design. For example, we rely on U.S. Global Positioning System (GPS) to provide position, navigation, and timing (PNT) services. GPS underpins navigation and emergency response and is key for U.S. military operations.[27]

---

[24] Jane Rickards, *Wary of Cable Sabotage, Taiwan Looks to Satellites as Back-ups,* The Strategist (Feb. 19, 2025), https://www.aspistrategist.org.au/wary-of-cable-sabotage-taiwan-looks-to-satellites-as-back-ups/.
[25] *See*, 2022 Communications Marketplace Report, Federal Communications Commission, at para. 174 (rel. Dec. 30, 2022), https://www fcc.gov/reports-research/reports/consolidated-communications-marketplace-reports/CMR-2022.
[26] Communications Act of 1934 § 2; 303 at 47 U.S.C. 152; 47 U.S.C. 303(r).
[27] John Plumb, *PNT Resilience for an Era of Great Power Competition*, CSIS (Oct. 31, 2024), https://www.csis.org/analysis/pnt-resilience-era-great-power-competition.

In recent years, Russia has warned that it could target commercial satellites.[28] Russia is publicly reported to be developing counterspace weapons, including potential nuclear anti-satellite capability. The impact of such weapons range from temporarily jamming satellite signals to permanently damaging components of satellites or even entire constellations.[29]

V. KEY QUESTIONS

- How do private sector providers mitigate risk and defend against cyber-attacks?
- How can the United States encourage innovation and maintain leadership in the satellite communications marketplace?
- How can the United States build redundancies into our networks and critical infrastructure?

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Kate Harper or Elaina Murphy of the Committee Staff at (202) 225-3641.

[28] Thomas Novelly, *Space Force on Notice as Russia Warns Commercial Satellites May Be a 'Legitimate Target*, MILITARY NEWS (Oct. 27, 2022), https://www.military.com/daily-news/2022/10/27/space-force-notice-russia-warns-commercial-satellites-may-be-legitimate-target.html.
[29] Dan De Luce, *Pentagon official warns Russian anti-satellite nuclear weapon could be devastating*, NBC NEWS (May 1, 2024), https://www nbcnews.com/news/world/pentagon-official-warns-russian-anti-satellite-nuclear-weapon-devastat-rcna150314.