Opening Statement for Chairman Richard Hudson
Subcommittee on Communications and Technology
"Global Networks at Risk: Securing the Future of Communications Infrastructure"
Wednesday, April 30, 2025 at 10:00 AM

Introduction

Good morning, and welcome to today's subcommittee hearing on Global Networks at Risk: Securing the Future of Communications Infrastructure.

This topic has never been more pressing. The United States is home to the world's leading companies and innovators who are driving the development of cutting-edge technologies like artificial intelligence, the Internet of Things, and next-generation wireless technologies. These innovations are critical not just to our economy, but to the future of global connectivity.

Communications are also central to our national defense. This is top of mind for me, especially as the Representative for Fort Bragg — home to the U.S. Special Forces and the largest military base in the

world. Connectivity and secure communications networks are vital to maintaining our defense capabilities and keeping our nation safe.

Today, we rely on communications infrastructure in nearly every sector of our economy. As Americans become more connected, it is increasingly important the equipment we buy and the networks we rely on are secure, resilient, and protected from malicious actors.

Unfortunately, the security of these networks is under threat.

The Chinese Communist Party (CCP), for example, has been investing heavily to develop unsecure communications equipment and export it around the world to assist in their espionage activities, including in the United States. The known vulnerabilities in many technologies produced by foreign adversaries pose a direct threat to the national security of the United States.

Last fall, we learned about Salt Typhoon, which may be the largest Chinese-backed telecommunications hack in our nation's history. These

hackers infiltrated U.S. telecommunications companies' networks, impacting at least nine providers. This infiltration enabled the hackers to "geolocate millions of individuals and record phone calls," and impacted senior U.S. officials, including then- President-elect Trump and Vice President-elect Vance.[1]

In addition to these vulnerabilities, there are an increasing number of physical attacks on communications infrastructure, such as undersea cables. These cables are responsible for carrying data traffic across oceans and are susceptible to damage by the elements and unintentional acts, such as anchors dragging along the seafloor. But they have also been intentionally sabotaged and because of their physical location under the ocean, it can be difficult to monitor unauthorized access to these cables.

[1] Rosie Perper, *Chinese hackers used broad telco access to geolocate millions of Americans and record phone calls*, Politico (December 27, 2024), https://www.politico.com/news/2024/12/27/chinese-hackers-telco-access-00196082

We must take decisive steps to address these threats. I was proud to support funding for the Secure and Trusted Communications Networks Reimbursement Program, which will support the removal of the remaining Chinese equipment in our communications networks.

Another key aspect of securing our communications infrastructure is the review of foreign investments in U.S. networks. "Team Telecom" is an interagency working group that reviews foreign investments in certain communications applications that come before the FCC.

Team Telecom assesses the national security risks, law enforcement, and other policy considerations that may be associated with such investments. While this process is important, applications often get bogged down by delays and bureaucratic hurdles. We must find ways to make sure that national security concerns are addressed without hindering deployment.

Satellite technology also plays an increasingly important role in our communications infrastructure. Satellites provide broadband services, as well as mission critical services to critical infrastructure companies and the Federal government. Yet the regulations governing satellite operations have not kept pace with the growth in the industry.

Last Congress, this committee led bipartisan legislation to streamline regulatory processes for satellite operators, and the Federal Communications Commission adopted many of these reforms. But more work remains to provide clarity and more certainty in the licensing process to ensure the U.S. remains a leader in this sector.

Conclusion

We must meet these challenges head-on. Innovation has provided untold benefits to Americans and to our economy. I look forward to hearing from the witnesses today about these issues.

I now yield five minutes to my colleague, Ranking Member Doris Matsui, for her opening statement.