Testimony by Laura Galante

Before the House Committee on Energy and Commerce, Subcommittee on Communications and Technology

On "Global Networks at Risk: Securing the Future of Telecommunications Infrastructure"

30 April 2025

Honorable Chair, Ranking Member, and esteemed members of this Committee, thank you for the opportunity to testify on the security of US telecommunications networks and their role in national security and US competitiveness.

My name is Laura Galante. I served as the Intelligence Community's Cyber Executive and the Director of the Cyber Threat Intelligence Integration Center (CTIIC) at the Office of the Director of National Intelligence (ODNI) from January 2022 to January 2025. Prior to this role, I led organizations that track, attribute, and expose cyber operations. I'll focus my remarks today on national security considerations for the US telecom sector.

The Telecommunications Sector in the Cross Hairs

This Committee recognizes that reliable and affordable telecom services form the backbone of America's digital infrastructure, enabling America's economic engine and global competitiveness.

The growth of the telecom sector has closely mirrored the digital transformation of our economy. Over the past 25 years, telecom companies have evolved from phone service providers into complex, multi-service digital organizations, navigating the convergence of communications, media, and technology. As with many tectonic digital shifts during this period, intelligence services have also become increasingly adept at targeting the immensely valuable data telcos manage through the vast network of digital roads they operate. In short, companies in this sector have become key targets for our foreign adversaries' operations.

Salt Typhoon: Beijing's Intelligence Operation against US Telecoms

Salt Typhoon marks a turning point. The operation, sponsored by the Chinese government and executed by contractors linked to Beijing's Ministry of State Security, was detailed publicly in Fall 2024 in media reports. They revealed that at least nine U.S. telecom and wireless communications companies were victims of extensive Chinese intelligence-gathering efforts.

In this multi-year operation, the actors breached multiple layers of major telecom networks, gaining unprecedented access to U.S. mobile communications across different carriers and various wireless technologies. This access enabled them to compromise the voice and text communications of top political figures and national security officials. Due to its sheer breadth and scope, this operation is regarded as the most expansive and consequential cyber espionage operation ever launched against the US.

Salt Typhoon presents three major issues that companies and governments will need to face:

1. **Increased Scale of Adversary Intelligence Operations:** Rather than focusing solely on the communications of specific high-value individuals, Chinese malicious actors breached and analyzed the complex operational networks of nine different telecom companies. This broad-scope approach underscored their intent to develop a durable, persistent intelligence capability that can support future objectives, rather than employing a task-specific, 'smash-and-grab' style operation.

2. **Delayed Detection of Salt Typhoon across the Telecom Sector:** Despite the telecoms' significant internal cybersecurity programs, detecting the Salt Typhoon compromise has required an extensive joint government-industry response. The ability to detect and rapidly remediate compromises against our most high-value networks must be a core capability for companies in this sector.

3. **AI Rapidly Expanding Data Processing Capabilities:** Rapid breakthroughs in AI have now equipped actors with powerful capabilities to make sense of large and disparate data sets that previously required immense time and resources to analyze at scale. These capabilities also enable even less sophisticated adversaries to extract key insights from vast amounts of data collected and merged from different industries and sectors.

Building a Secure Future

The hard question this Committee faces is how to strike a balance between securing the digital roads of our economy and everyday life with the enormous, growing demand for fast and affordable digital connectivity.

We can't regulate our way to an enduring answer. The technology changes too quickly, and the ingenuity of our adversaries is relentless. But we must build a better, more dynamic operational security model than what we have today. This model will require bringing the threat intelligence and national security expertise of the Intelligence Community together with key private sector representatives in the telecom and secure technology sectors. This intelligence-driven approach should then drive operationally-sound practices that companies implement across their infrastructure.

The good news is, we've done this before. One of the mechanisms available to drive this process–until it was dissolved last month–was the Enduring Security Framework founded in 2007. This was a partnership run by the National Security Agency along with the Office of the Director of National Intelligence, and it operated under the authorities of the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council (CIPAC). The Enduring Security Framework proved successful enough that both the British and Australian intelligence services used it as the model for their own highly regarded national cyber centers.

Serious security practitioners in government and industry alike used the now-dissolved Enduring Security Framework along with other CIPAC boards including the Cybersecurity Review Board (CSRB)--also dissolved–to convene and work through hard tech security challenges and develop solutions. The CSRB, similar to the National Transportation Safety Board, investigated major cybersecurity incidents, like Salt Typhoon. These joint efforts developed evidence-based approaches to address major security breaches and threats in coordination with the private sector entities responsible for securing our critical infrastructure.

This collaborative security and intelligence work has been America's differentiator in the global secure technology market. It is an ecosystem of security professionals, intelligence officials, analysts, and operators that track vulnerabilities and threats as quickly as they spread and deploy patches, fixes, and new security paradigms.

Dismantling this public-private security ecosystem will weaken our collective defense and national security posture. A risk, I believe, we can't afford to take.

I look forward to your questions.