Testimony by Laura Galante

Before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party

On "End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses"

5 March 2025

Honorable Chair, Ranking Member, and esteemed members of this Committee,

Thank you for the opportunity to testify on the People's Republic of China (PRC)'s cyber operations–an issue of critical importance to US competitiveness and national security.

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 through 2025. In my prior private sector roles, I worked extensively on tracking, attributing, and exposing malicious cyber operations. I look forward to providing insight on the evolution of the PRC's cyber program, particularly in light of the unprecedented operations against US telecommunications ("telecoms") providers.

In fall 2024, US media reported that numerous US telecoms and other wireless communications companies were victims of an extensive PRC-sponsored intelligence operation. Dubbed "Salt Typhoon," PRC actors had breached multiple layers of at least nine major US telecoms' networks. This gives the PRC wide access to US mobile communications across carriers and across different wireless communication technologies. This operation is the most expansive and consequential cyber espionage operation ever launched against the US.

The targets of this operation–US telecommunications providers–secure some of the most complex and high value networks and infrastructure. In 2023, the Director of National Intelligence warned that "China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."

Telecom providers operate multiple technology stacks: from the literal physical "pipes" of the internet up to the customer-facing services like texting and calls. Telecommunications technologies have also dramatically evolved over the last twenty years, yet companies still maintain many legacy networks and technologies. Despite the telecoms' significant internal cybersecurity operations, detecting Salt Typhoon's compromise has required an extensive joint government-industry response. The US government issued a series of advisories and guidance to help companies identify Salt Typhoon activity in their networks.

The people behind this operation are a group of contractors who work for China's Ministry of State Security (MSS). In January, the Department of Treasury sanctioned Sichuan Juxinhe Network Technology Co., LTD. (Sichuan Juxinhe) citing their "direct involvement in the exploitation of these U.S. telecommunication and internet service provider companies. The MSS has maintained strong ties with multiple computer network exploitation companies, including Sichuan Juxinhe."

The Ministry of State Security, among other functions, handles the PRC's counterintelligence, espionage, and political security. The MSS–like other state Chinese cyber operators–relies on a network of companies that perform research and development tasks that serve as the basis for compromising vulnerabilities in network configuration and security products. These companies frequently change names, alter their corporate structures, and take other steps to avoid detection and scrutiny. This ecosystem of Chinese IT and cybersecurity contractors remains largely intact and undeterred by US sanction efforts and a widely publicized 2024 leak of the inner-workings of a contractor called "I-Soon."

The Salt Typhoon operation demonstrates that this outsourced model–where contractors can achieve major espionage objectives against complex, high-value victim networks–gives China a well-honed and effective capability to scale the PRC's foreign network operations. It provides the PRC with a competitive marketplace for network exploitation capabilities and outsources the most sensitive target development and operations–like those against US companies. This, in effect, minimizes the risk of exposing larger state espionage and attack plans.

Salt Typhoon's success in compromising multiple parts of the US telecommunications' architecture builds on over a decade of bulk as well as targeted cyber espionage operations against the US. In 2015, PRC actors compromised the Office of Personnel and Management and obtained more than 21 million former and current government employees' Social Security Numbers, addresses, and other data points. In 2023, the PRC successfully breached the Department of State and Microsoft in order to collect on the communications of senior US officials involved with US-China policy, including the US Ambassador to China and the US Secretary of Commerce. These are just a few examples of the types of personal data and operations that give the PRC–and in turn, its enabling companies–ample proof points to refine effective operations against the US.

To understand where the PRC is going with this capability, we need look no further than the domestic surveillance apparatus that President Xi has invested in and refined over the last decade – against the Chinese people. The DNI put it succinctly in 2023: "China leads the world in applying surveillance and censorship to monitor its population and repress dissent." As the PRC refines its tools and methodologies domestically–particularly with the application of recent AI advances–we should expect them to harness and deploy these capabilities against the US, our allies, and nations critical of the PRC.

Thank you. I look forward to the discussion today and your questions.