Statement before the
Senate Committee on Commerce, Science, and Transportation
"Strategic and Operational Concerns Raised by the SALT TYPHOON Intrusions,"

A Testimony by:

James Mulvenon, Ph.D.
Chief Intelligence Officer
Pamir Consulting

December 11, 2024

Russell 253

Introduction and Main Points

Chairman Cantwell, Ranking Member Cruz, and distinguished members, thank you for inviting me to testify today.

I have been researching Chinese cyber operations since the mid 1990s. The SALT TYPHOON cyber campaign by PRC state actors is the most serious telecommunications compromise I have seen in my career, raising a range of strategic and operational issues that fall under the jurisdiction of this Committee.

The Strategic Cyber Deterrence "Hole" is Getting Deeper

- The United States is currently in a deep deterrence "hole" with respect to China.
- Neither Beijing (nor Moscow or Tehran for that matter) believe that they have found America's "pain point" regarding cyber intrusions or attacks, further emboldening them to conduct deeper and more dangerous penetrations.
- Much as we would like, we can't simply declare today that we have a credible cyber deterrent; it must be recognized by others as credible.
- Deterrence comes in at least two distinct forms, deterrence by punishment and deterrence by denial.
- Cyber deterrence through denial is primarily based on computer network defense, but it is cost-prohibitive, as cyber offense, which only needs to find one way in, is demonstrably cheaper than cyber defense, which must prevent every avenue of entry. Given the nature of the network, deterrence through denial therefore seems to be extremely difficult.
- Deterrence through punishment, by contrast, is primarily an offensive game, based on the threat of credible and painful retaliation for adversary attacks; in other words, imposing costs. In the cyber realm, deterrence by punishment theoretically offers better chances of success, especially against adversaries that have well-developed cyber infrastructure.
- Some progress was made in the first Trump Administration, particularly its promulgation of NSPM-13 "United States Cyber Operations Policy," which clearly articulated a "bias for action" and for the first time lowered the threshold for authorization of offensive cyber operations by delegating "well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace."
- The current dynamic with China in cyberspace will not change unless a similar, and hopefully even more forward-leaning policy like NSPM-13 is enacted in the new administration.

The Operational Concerns about Federal Wiretapping and Collection are Gravely Serious

- According to public reports, the Chinese intruders gained access to the systems used by the carriers to comply with wiretapping and FISA Section 702 requirements, potentially exposing the targets of U.S. law enforcement and intelligence collection and undermining related counterintelligence operations.
- This is not the first time Chinese intruders have penetrated these types of systems. Public reports asserted that China's Operation Aurora campaign in 2009 against Google also breached their FISA Section 702 systems.

- Public reports suggest that the Chinese intruders used a vulnerability in the existing infrastructure hardware that cannot be remediated and would require a generational upgrade of equipment costing billions of dollars.
- The CALEA (Communications Assistance for Law Enforcement Act) law, especially Section 105 "Systems Security and Integrity," provides ample basis for the Committee to mandate the carriers provide a detailed remediation plan for the vulnerability.
- The recent FCC announcement citing Section 105 as the basis for a Declaratory Ruling that "would require communications service providers to submit an annual certification to the FCC attesting that they have created, updated, and implemented a cybersecurity risk management plan" is not nearly proactive enough.

The "Rip and Replace" of the Vulnerable Hardware Could Be a Huge Boon for Domestic Telecommunications Equipment Manufacturing

- American telecommunications equipment manufacturers like Cisco and Juniper have struggled for decades to meet the challenge from unfairly subsidized competitors like Huawei and ZTE.
- A massive overhaul of the U.S. core infrastructure, restricted to trusted Western equipment manufacturers, would be a huge boost to domestic manufacturing.