Statement before the Senate Committee on Commerce, Science, and Transportation
Subcommittee on Communications, Media and Broadband

"Communications Networks Safety and Security"

A Testimony by:

James Andrew Lewis

Senior Vice President; Pritzker Chair; and Director, Strategic Technologies Program, CSIS

December 11, 2024

253 Russell Senate Office Building

Chairman Luján, Ranking Member Thune, distinguished Members of the Subcommittee, I'd like to thank the Committee for the opportunity to testify.

Let me thank the Committee for the opportunity to testify on one of the most pressing strategic problems facing the United States, the security of the U.S. telecommunications system. This kind of problem is not new. In 1863 the Secretary of State warned the United States' representative in France that messages sent to Washington over telegraph networks were being read. In 1900 Britain's dominance of the first global networks gave it strategic advantage. In the 1980s, the Reagan Administration gave senior officials special "white" phones to protect against ubiquitous Soviet telecommunications surveillance. While China's actions are not new, the scale of our dependence on global networks and audacity of Chinese communications espionage is unprecedented.

All great powers engage in communications espionage. The United States itself is no slouch in this regard, something the Chinese will happily point out if you discuss it with them. The internet has made communications espionage even easier and for the last decade, the problem for major intelligence agencies became not just to acquire information but to find ways to store and analyze it, given the vast quantities involved.

The global telecommunications network is comprised of satellites, undersea cables, terrestrial fiber optics, and wireless networks. This includes devices connected to the internet, cloud services, and the hardware and software that make up the telecommunications infrastructure. These are all interconnected and vulnerable, making this the golden age of communications intelligence. The mobile phone is a gift to spies. A wealthy and hostile nation like China can afford to exploit them all with programs that target space assets, undersea cables, and telecommunications infrastructures, all accompanied by extensive efforts at hacking internet-accessible assets.

Chinese espionage began shortly after the opening of the Chinese economy to the West. Chinese cyber espionage began around 2003 when it built high-speed connections to the new internet. Suddenly, the poorly protected data and networks of U.S. companies, universities and government agencies became easily accessible to China's cyber spies.

There are many examples of this. China leads the world in espionage-related hacking against the United States. Telecommunications has always been a part of this. Beginning more than two decades ago, large scale Chinese government support for Huawei provided both commercial and intelligence benefits, and embedded China in the telecommunications infrastructure of many strategically significant countries, giving it access and potentially control of vital networks. And several years ago, there were incidents involving China Telecom, when it diverted massive amounts of internet traffic to pass thought China where it could be collected. The famous spy balloon incident was most likely an effort to collect mobile telephone communications (among other things). China is also active in other intelligence areas, such as the use of clandestine agents and satellites, but communications espionage is their centerpiece.

The Chinese have had some remarkable successes against the United States, most recently with what some call 'Salt Typhoon.' This is only the latest Chinese effort, affecting more than two

dozen countries. Investigations into the scope and damage are still ongoing. It is premature to say the full effect has been understood or remedied or what, if anything, the Chinese may have left behind on the networks they penetrated. Salt Typhoon should not be seen as an isolated incident but as part of a larger Chinese campaign to systematically exploit global telecommunications networks.

Judging from initial reporting on Salt typhoon, the operation would allow China to be able to see Foreign Intelligence Service Act (FISA) intercept orders submitted to U.S. telecommunications companies, showing which of its agents had been detected (as well as anyone else the United States was interested in surveilling). And while it is unclear what other data China obtained with Salt Typhoon, there are reports that it acquired metadata and content from numerous high value U.S. targets by accessing their telephone calls and texts messages. Everyone on this Committee is a target.

It is also likely that Salt Typhoon has elements that go beyond espionage. An earlier incident named by some companies as "Volt Typhoon" saw China preposition malicious code on U.S. critical infrastructure networks. Salt Typhoon may have also been used in prepositioning malicious code on telecommunications networks. Prepositioning goes beyond espionage as it is a precursor to attack.

To understand and counter China, we must consider the whole picture and not just a single aspect. China has constructed a broad global signals intelligence (SIGINT) surveillances system. China often "mirror images" or copies what it thinks the United States is doing. The model China is copying here is sometimes called "Echelon," which in the vivid imaginations of those hostile to the United States is a global system for intercepting all digital communications. This is inaccurate, but China tries to go one better than the United States and it has different tools, such as state control of telecommunications equipment manufacturers, which it is using to build a global communications espionage network where the United States is the primary target.

From the outside it appears that China has a comprehensive strategy for cyber espionage and communications intelligence that began soon after China gained access to the internet more than two decades ago. For years, the United States accepted this as the cost of doing business in China. China's initial focus was on commercial and technological espionage as well as conventional politico-military espionage. In the last decade it has expanded in both scale and scope to include preparing for disruptive actions against critical infrastructure including telecommunications networks, monitoring and coercing Chinese citizens who are resident in the United States, and collecting reams of personal data from American citizens. Access to the U.S. telecommunications network is vital to all these efforts.

Huawei remains the exemplar of this effort. It first benefited from the theft of technology (although it no longer needs this as much). It still benefits from immense subsidies from the Chinese government, and these helped it drive Western competitors out of the telecommunications infrastructure business and left it as the major supplier of network infrastructure (in terms of deployed networks) around the world. It was a brilliant strategy that has made China dominant in global telecommunications networks in the way that Britian dominated them 120 years ago. Huawei's success makes 'rip and replace' even more important

and its inclusion in the National Defense Authorization Act (NDAA) for eventual passage is an important step for which the Committee is to be congratulated.

Countering China requires two sets of actions. The first is to begin a sustained, direct, and more forceful effort to disincentivize Chinese espionage. The second is to accelerate and expand efforts to harden our own networks and, if possible, those of allies. The United States' response has been too restrained. Economics have outweighed security, something the Chinese count on to hobble the U.S. response. China faces no real penalty for espionage and the traditional remedies have been insufficient. One of the most serious drawbacks for U.S. strategy is a reluctance to actually engage directly and effectively with hostile actors. As our opponents become more brazen in their actions, a reliance on limited and reactive measures guarantees that hostile actions will only increase. This is the unpleasant reality in which the United States finds itself.

None of the traditional counter-espionage remedies, which are intended to signal displeasure to an opponent and persuade them to reduce their actions, have worked. Expelling diplomats, arresting spies, even closing a Chinese consulate has not persuaded China to scale back. Until recently, the United States and its allies were largely supine in the face of Chinese espionage. The one exception to this was the 2015 intervention by President Obama after the OPM hack, but the effort was short-lived and reportedly even opposed by some of his staff.

Finding an appropriate and effective response to aggressive Chinese espionage is one of the central diplomatic and foreign policy challenges facing the United States. Deterrence in cyberspace has been a complete failure. Developing a program of active defense with our allies is essential for changing China's behavior. What has been done so far, largely the occasional complaint, is insufficient. More assertive measures could include political campaigns to exert pressure on China's leaders, operations to interfere with opponent cyber capabilities, or more comprehensive and damaging sanctions (an approach that European allies would find more acceptable). When China complains about tariffs, it could be useful to remind them of the need to change their behavior.

This is a complicated issue as there is some risk of increased conflict and the Chinese will respond vigorously, perhaps by threatening to use their market leverage. It comes at a time when bilateral relations will become even more difficult, but the damage from accepting Chinese espionage has grown to the point where it is a major security risk, if only because it suggests to the Chinese that the United States will fail to respond to other provocations matter how grave.

Instead, the United States has focused on hardening its defenses. In themselves, these efforts are valuable although still insufficient. As we improve the security of U.S. telecommunications defense, some less sophisticated opponents will be unable to overcome these defenses. Unfortunately, China is not one of them. While our patchwork efforts to build resilience and security make the task of surveillance more difficult and expensive and is a necessary step, China has the resources and commitment to prevail.

Interagency disputes hamper the hardening of networks, and it should be made clear that the Federal Communications Commission (FCC) is the regulatory agency in charge (and regulation is necessary since the alternative has been shown many times to be inadequate for cybersecurity).

This may not require new legislation, but it will require Congressional oversight. The FCC has taken action, but more is needed.

In 2022, the FCC banned new telecommunications equipment from Huawei, ZTE, and other Chinese firms, citing national security concerns. This was under the agency's "Covered Equipment Authorization" rules. In 2022 it also revoked authorizations for China Unicom Americas, China Telecom Americas, and Pacific Networks and its subsidiary ComNet to provide telecommunications services in the United States as these gave China a presence on U.S. telecommunications networks. In 2021, the FCC implemented rules requiring carriers to remove and replace existing equipment from these companies in what is known as the 'rip and replace' program. Rip-and-replace by most accounts is 80% complete, making continued progress essential.

The recent FCC effort to use CALEA (Communications Assistance for Law Enforcement Act) authorities to require telecommunications companies to meet cybersecurity requirements could, if carefully constructed, usefully improve defenses. CALEA calls on telecommunications carriers to protect intercept controls and data from unauthorized access, implement access controls and audit mechanisms, and ensure the secure transmission of intercept data to law enforcement.

There is an easy comparison between the effort and resources banks put into cybersecurity versus the amount spent by telecommunications companies. Publicly available documents suggest that on average, major banks spend between 6-12% of their IT budgets on cybersecurity compared to 3-5% spent by major telecommunications companies. Major telecom firms do take cybersecurity seriously but may not fully match the depth and resourcing of efforts in the financial sector.

Major U.S. telecommunications companies could strengthen cybersecurity through infrastructure modernization, use of zero-trust architectures, and increased network segmentation. Copying the financial sector practices, they could improve their threat detection by deploying advanced monitoring tools, AI-based anomaly detection, and automated incident response. Stronger access controls and robust identity management would help. Telecommunications companies could invest more in acquiring cybersecurity talent and expanding security teams. The challenge is balancing these improvements against operational requirements and costs.

As the Committee knows, telecommunications modernization comes in regular cycles. We are now at the in the midst of the latest cycle to the next generation of telecommunications (5G) and the greater use of Open Radio Access Networks (ORAN). This transition offer an opportunity to remedy some of the technical vulnerabilities that China exploited for Salt Typhoon, but 5G and ORAN and their reliance on cloud services also increase the need for improved cybersecurity.

There is always a cost to regulation and it would be best if decisions on regulation and best practices were informed through a consultative process led by the Office of the National Cyber Director (ONCD). ONCD should work with the telecommunications, cloud, and financial sector companies to identify additional steps and cooperative measures to improve the security and resilience of the national telecommunication infrastructures.

Despite some good work, not enough has been done and the Committee can perform a valuable service by changing this. It can make clear that the FCC is the regulatory agency in charge (and judging from the financial sector experience, regulation is necessary). This Administration has taken several steps to improve cybersecurity and hopefully the next will continue them. Securing telecommunications networks must be a higher priority. A reliable, resilient telecommunications infrastructure is essential for security and economic strength, and this requires minimizes the opportunities for communications collection by adversaries and putting China on notices that its actions will no longer be tolerated without penalty.

China had a comprehensive strategy (to exploit communications) and the United States does not have a comprehensive strategy to defend them. The advantage lies with our opponents and the work of this committee can help change that. Thank you for the opportunity to testify.