# Testimony by Rob Joyce

# Before the House Select Committee on the Chinese Communist Party

# 5 March 2025

# Cannon House Office Building.

**Opening Statement**

Honorable Chair, ranking member and distinguished members of the Committee, thank you for the opportunity to appear before you today. I am Rob Joyce, the former Director of Cybersecurity at NSA where I served for 34 years. I was also the White House Cybersecurity Coordinator and acting Homeland Security Advisor. I want to address what I consider the most significant cybersecurity issue facing the United States: the multifaceted cyber threats emanating from the People's Republic of China (PRC).

The PRC is conducting a comprehensive cyber campaign against the United States, and our current defenses are not keeping pace. Chinese state hackers prepositioned malware within our power grids, pipelines, water treatment plants, and other critical infrastructure. They tapped into our telecommunications to spy on us, stole the innovations of technological research and breached the cloud systems holding government emails. They even unfairly exploit our open markets to achieve a growing advantage inside the technology we rely upon for our communications. After a decade of using cyber to steal industrial and military secrets, they've evolved to far more threatening penetrations of our nation's infrastructure. They run cyber operations deliberately intended to create "societal panic" at the time of escalating tensions. Planning cyber terrorism is a direct threat to our national security and economy.

The PRC is not only using cyber operations to their advantage, they are undercutting our market to deliver Chinese-controlled technologies into our homes, raising significant national security concerns. TP-Link, the world's largest manufacturer of commercial Wi-Fi and home routers has grown to at least 60% of the U.S. retail market for Wi-Fi systems and SoHo routers compared with about 10% of the market at the start of 2019. How have they achieved this miraculous growth? They appear to be selling at price points below profitability to drive out the western competition. As of August of 2024, TP-Link captured nearly 80% of the US retail market for mesh systems running on Wi-Fi 7, the newest Wi-Fi specification in existence today. TP-Link routers were among the various brands exploited by Chinese state-sponsored hackers in the massive Volt, Flax, and Salt Typhoon attacks. Imagine these routers in the homes and businesses across America as a PRC platform to launch society-panicking cyber attacks during an invasion of Taiwan. We cannot have the software for these prolific devices be written, updated, and controlled by a Chinese company. By law, such a company is subject to the direction of the PRC Intelligence apparatus. This is a threat we cannot ignore.

I know this hearing isn't simply about the problems we face; it is important to discuss solutions that keep us safe. There are three pillars of work we must focus on:

First, we must improve our tools to deter these PRC actions. Deterrence is not an abstract concept—it requires making it clear to everyone in the chain of command, from the individual hackers to military generals and Politburo leadership, that the costs of these cyber operations outweigh any potential benefits. While strengthening our cyber defenses is essential, this alone will not change their behavior. No single approach will achieve effective deterrence; instead, we need a comprehensive campaign that imposes costs across multiple dimensions. This integrated arsenal should include offensive cyber operations to disrupt their capabilities, targeted economic sanctions, public indictments, coordinated international law enforcement actions, diplomatic pressure, export controls, and intelligence sharing with industry and allies. Overall, we must include high-level political engagement to establish clear expectations for acceptable online behavior, coupled with concrete demonstrations that violations will have meaningful consequences.

Second, we need stronger defenses. Too often, attackers exploit well-known vulnerabilities that remain unpatched. Robust cybersecurity comes at a cost. Too much of our critical infrastructure doesn't have the investment and rigor needed to protect us. Industry also leaves too many flaws in the software we rely upon. There are certainly levers that can drive more security into the ecosystem, and we must use them. This includes eliminating TP-Link's footprint from our nation and ensuring other PRC capabilities are not enabled in our infrastructure. Part of the defense is also having expertise and capacity in the government. I want to raise my grave concerns that the aggressive threats to cut US Government probationary employees will have a devastating impact on cybersecurity and national security. At my former agency, remarkable technical talent was recruited into developmental programs that provided intensive training and hands-on experience to cultivate vital skills. Eliminating probationary employees will destroy a pipeline of top talent, essential for hunting and eradicating PRC threats. Even if they are not eliminated, the pervasive uncertainty and doubt in the current environment are forcing them to seek secure opportunities for their families outside national security. The uncertainty is also discouraging future cybersecurity talent from joining our ranks. In short, the most talented individuals will no longer choose to serve at NSA, CISA and other federal positions. I implore you, in the strongest possible terms, to consider the catastrophic consequences that this indiscriminate and unfocused pressure will have on the competency and capability of the men and women dedicated to safeguarding our nation. We need this talent to win in competition and conflict.

Finally, assuming our adversaries still come at us, and our defenses improve, we must still plan to be resilient. We must ensure cyberattacks have limited impact, quick recovery, and minimal disruption. There are mitigations that must be made to reduce our exposure, even when hacks are successful.

I look forward to exploring these concepts during your questions.