Testimony by Rob Joyce

Before the House Subcommittee on Cybersecurity, Information Technology, and Government Innovation

On "The Threat to Our Nation's Critical Infrastructure Posed by Cyberattacks from the People's Republic of China"

15 May 2024

Rayburn House Office Building.

Honorable Chair, Vice Chair, and esteemed members of this Subcommittee,

Thank you for the opportunity to appear before you today and discuss what I consider the most significant cybersecurity issue faced by the United States. This is the threat that cyberattacks from the People's Republic of China (PRC) pose to our nation's critical infrastructure. My name is Rob Joyce. I served over 34 years at the National Security Agency, retiring as the Director of Cybersecurity. I hope to provide insight into the sophistication and strategic implications of these PRC cyber threats and how they compete fiercely in the cyber domain.

It is widely understood that for years, PRC hackers have stolen intellectual property to aid their domestic industry. Chinese state-sponsored hacking groups like APT41 have systematically conducted cyber espionage campaigns to steal trillions of dollars worth of intellectual property and trade secrets from U.S. companies across critical sectors like aerospace, pharmaceuticals, energy, manufacturing and more. For example, a multiyear campaign was uncovered in 2022 where APT41 infiltrated over 30 multinational firms and exfiltrated hundreds of gigabytes of proprietary data - including designs for fighter jets, missiles, drugs, solar panels, and other cutting-edge technologies not yet patented. Such brazen theft robs American companies of their R&D investments and competitive advantages, undermining U.S. economic interests. The annual cost to the U.S. economy from IP theft is hundreds of billions of dollars and does not include the long-term impact when China illicitly closes technology gaps and brings competing products to market using stolen information.

We have also seen examples of cyber intrusions for the purpose of traditional espionage. In 2023, the U.S. State Department discovered the compromise of its emails system. The attackers accessed the inboxes of the U.S. Secretary of Commerce, the U.S. Ambassador to China, and key State Department employees working on East Asia matters before a sensitive visit by the Secretary of State to China. Microsoft assessed the intrusion was the Chinese threat actor they call Storm-0558, and according to the Cyber Safety Review Board study on this event, the activity was so stealthy that Microsoft still can't say with certainty how the credentials used in the attack were stolen from them.

The issues of espionage and intellectual property theft have persisted for years, but we are here to talk about an even more troubling set of cyber intrusions. 2023 saw the U.S. cybersecurity

community develop an increased understanding that a set of PRC hackers labeled Volt Typhoon was prepositioning on U.S. Critical Infrastructure. They were not there to steal information, but instead they prepared to disrupt vital critical infrastructure systems. They wanted to slow the U.S. military's ability to mobilize and deploy in the time of crisis. They also wanted the capability to sew societal panic at the time of their choosing. They wanted to be able to turn us inward and focus on serious critical infrastructure problems at home rather than supporting any crisis on the other side of the globe. There's a simple description for their intent: domestic terrorism. They wanted the general society to be afraid because of the effects they delivered in cyberspace. That is serious and disturbing.

This activity was discovered and validated through a unique collaboration of government and industry. Foreign intelligence was used in conjunction with the tremendous insights of industry. In May of 2023, my former agency, NSA, along with multiple government agencies, both domestic and international, described these intrusions in a public cybersecurity advisory. If you read the advisory, you will also see 11 of the biggest internet and telecommunications companies added their names to the publication as participating in the investigation.

Subsequent work by FBI, CISA and industry has confirmed Volt Typhoon compromised the IT systems of diverse critical infrastructure sectors including Communications, Energy Transportation and Water and Wastewater Systems. We've found prepositioning of these activities in the continental United States, as well as the U.S. territory of Guam. The intrusions in Guam are significant because the island hosts Andersen Air Force Base, and Naval Base Guam, which are the major U.S. military outposts that would play a crucial role in any potential conflict with China over Taiwan.

The intrusions have gone on for quite some time but have generally escaped notice. The hackers don't bring custom malware to the compromised networks. They generally steal the identities of legitimate users, allowing them to blend into the expected traffic of the network. Sometimes, they create new users to infiltrate the systems more stealthily. Because of this tradecraft, known as "living off the land", antivirus and other defensive techniques won't alert on the intrusions, making them very hard to discover. Additionally, because the hackers are not there to steal information, the traditional tripwires looking for large volumes of information leaving a network are ineffective. The hackers camouflage their activity within normal network operations, making periodic intrusions to ensure they maintain access—thus evading typical detection methods. It is the height of stealthy operations. Another part of their tradecraft makes the intrusions hard to find. The hackers do not connect to their targets directly from China, but instead, move through a series of hacked or leased computers to obfuscate their origins. Often the last hop of the chain is the small box that cable companies and internet providers place in the homes of their customers to provide service. These devices are compromised and incorporated into botnets, which enable the PRC hacking operations, which presents an additional challenge because the communications are now U.S. based and subject to our legal regime for collection.

Despite all these stealthy traits, a coalition of sophisticated defenders was able to come together to uncover and illuminate the intrusions. The first public report of this hacking activity in May of last year specifically named eleven major internet and cybersecurity companies that were working with NSA's Cybersecurity Collaboration Center where foreign intelligence was combined with insights

from the company's own data to understand more together than any of us could know alone. Since that point in time, even more have joined the effort. Our strength in pursuing these intrusions lies in the unique data, capabilities, and expertise that each participant brings.

I'll conclude by noting that in January of this year, there was a hearing before the House Select Committee on Strategic Competition between the U.S. and the CCP, which included the Director of FBI, the Director of NSA, the Director of CISA and the National Cyber Director. Each talked about how the critical infrastructure that underpins the economic, security, and social well-being of the United States is increasingly under siege. It is my experienced understating that these attacks on our critical infrastructure are not just incidents of cybercrime or espionage; they are deliberate and calculated strategies employed by the Chinese government aimed at destabilizing our confidence and willingness to help maintain the peaceful world order. These deliberate strategies by the Chinese government to destabilize our confidence warrant your full attention and support, ensuring the PRC cannot undermine our national security.

I look forward to answering your questions alongside this knowledgeable panel.