Testimony of

Rocky Cole
Co-Founder & COO of iVerify

Before

House of Representatives
Committee on the Judiciary
Subcommittee on Oversight

“Embedded Threats: Foreign Ownership, Hidden Hardware, and Licensing Failures in America’s Transportation Systems”

January 21, 2026

Chairman Van Drew, Ranking Member Crockett, and distinguished members of the Committee, thank you for the opportunity to testify on threats to America’s critical infrastructure, many of which are hiding in plain sight.

I’ve worked to counter America’s top cyber adversaries for almost twenty years now, first within the United States Intelligence Community, then at Google, and now at a U.S.-based, venture-capital backed company called iVerify, which focuses on securing the highly sophisticated computers we all keep in our pockets, mobile devices. I’ve witnessed the strategic evolution of cyber operations, from the early days of cyber espionage to today's Cyber Cold War, and my experiences have informed a unique perspective on both the problem and steps we can take to mitigate these threats.

The topic of this hearing is embedded threats in America’s transportation systems, and I plan to address those directly; however, these threats are best understood in the broader context of America’s critical infrastructure, as they constitute one piece of a larger strategic landscape.

Historically, both Chinese and Russian cyber operations were focused on intelligence gathering. For the PRC, this meant extracting intellectual property to feed their “Made in China 2025” strategy, while Russia focused on political interference. However, we have reached a watershed moment where the objective has shifted to pre-positioning for disruptive effects. Modern doctrine now views cyberspace as a basic platform for hybrid warfare, where blinding cyberattacks are intended to paralyze command and control networks before kinetic operations even begin. U.S. intelligence assesses with high confidence that these actors are embedding "sleeper software" within our infrastructure to be activated at will.

Today, the United States faces a sophisticated doctrine of strategic pre-positioning within our critical infrastructure by our key adversaries. This evolution represents a transition from opportunistic data theft and political espionage to the systematic infiltration of the systems that underpin modern life—including our telecommunications, energy, water, and yes, transportation

networks. By embedding themselves in these sectors, these actors have created a persistent threat designed to support kinetic military operations during future crises.

The threat from China is particularly acute through several multi-year campaigns aimed at achieving "information dominance." The Volt Typhoon campaign targets energy, water, and transportation sectors specifically to disable military mobilization and to sow domestic chaos that would distract U.S. leaders during a potential invasion of Taiwan. Furthermore, Salt Typhoon has compromised the "backdoor" systems used by telecommunications providers for court-ordered wiretapping, allowing the PRC to monitor law enforcement, track the real-time geolocation of millions of Americans, and compromise mobile phones. Their operations have even expanded to targeting toll systems through SMS phishing and compromising state-level commercial driver's license databases, which are vital for our national logistics.

Simultaneously, Russia continues to integrate cyber operations directly into its military campaigns, using Ukraine as a testbed for destructive tactics. Their Sandworm unit, considered the apex of destructive state-sponsored hacking, has integrated "wiper" software designed to ruin industrial control systems in the energy and telecommunications sectors. Since 2022, they have also conducted sustained reconnaissance on air, sea, and rail transportation to disrupt the delivery of assistance to Ukraine. These state actors are further supported by affiliated hacktivists who perform opportunistic attacks on U.S. water and energy infrastructure by capitalizing on unsecured network connections.

To evade detection, these actors have refined their methods to bypass modern defenses through "malware-free" intrusions. They utilize "Living off the Land" techniques, using legitimate system administration tools to blend in with normal activity and avoid detection. They rapidly exploit high-severity vulnerabilities in firewalls and VPNs within days of disclosure and increasingly target less-monitored devices, like employee mobile phones, to steal credentials. Furthermore, they hijack domestic consumer infrastructure, such as end-of-life routers and internet-of-things devices, to create operational relay networks that mask the origin of their traffic.

And finally, as per the topic of this hearing, they increasingly utilize supply chain operations to gain backdoor access to critical technologies. This can manifest as tampering with or implanting hardware components, inserting malicious code into software updates, or compromising the integrity of manufacturing processes for devices like routers, servers, and even large industrial equipment such as port cranes.

Despite the magnitude of the threat, the United States remains hamstrung by a patchwork regulatory landscape and structural challenges that impede a unified defense. Our defensive posture is characterized by voluntary frameworks that have failed to keep pace with the adversary's strategic pivot to pre-positioning. Compounding this, the complexity of coordinating between federal and 50 state-level regulatory bodies creates systemic gaps that adversaries readily exploit. On the offensive side, limited authorities and an over-reliance on dated international norms have often restricted the efficacy of U.S. cyber operations, allowing adversaries to operate from sanctuaries with relative impunity.

This asymmetry demands a significant structural and legal overhaul to achieve true cyber deterrence.

This includes formalizing the authority to "Defend Forward" by disrupting adversarial groups within foreign networks before they reach the homeland. We must also address systemic personnel failures within the United States Cyber Command by transitioning toward an independent Cyber Force that establishes uniform standards for recruitment and training, bypassing traditional military standards that often hinder cyber readiness. Most importantly, we should consider advancing a framework that treats cyberattacks on critical infrastructure that imperil human life as acts of war equivalent to kinetic strikes.

We must also harden our domestic resilience by moving beyond voluntary standards. Congress should fund states to build high-maturity response capabilities and convert voluntary security goals into mandates for systemically important entities, requiring redundant power and physical hardening across all critical sectors. We must shift the legal "duty of care" to software manufacturers and away from end-users, holding them liable for design flaws while mandating a move to “Secure by Design” principals, rather than today’s voluntary pledges. And finally, to mitigate supply chain risks, Congress must implement mandatory screening and eventual phase-out of Chinese-manufactured hardware with remote communications capabilities within highly sensitive critical infrastructure and federal networks, akin to the rip-and-replace campaigns Congress funded to remove Chinese-made telecommunications gear from America’s core networks.

In conclusion, we must assume that our adversaries maintain persistent access to many of our critical systems. Reclaiming the operational advantage requires a unified strategy that fuses regulatory, industrial, and diplomatic efforts. While the U.S. moves toward "preemptive erosion" to hold adversaries' infrastructure at risk, we must simultaneously harden the home front through institutional reform and mandatory technical standards. Only through this combination of defending forward and securing the home can we hope to deter this latent threat from escalating into active, widespread disruption.

Thank you, and I look forward to your questions.