JOE LIN WRITTEN TESTIMONY

Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland"

Tuesday, January 13, 2026

Chairman, Ranking Member, and Members of the Committee,

Thank you for the opportunity to speak before you today. My name is Joseph Lin. I am the CEO of Twenty, the first U.S. venture-backed cyber warfare start-up, building industrial-scale offensive cyber capabilities for the United States and its allies. I've spent my career working alongside the Intelligence Community, the Department of War, and civilian agencies defending American networks.

My co-founders and I founded this company for a simple reason: America is under sustained cyber attack, and our adversaries have learned—correctly—that those attacks rarely produce consequences. We decided to change that—by making our adversaries think twice before they attack us.

For too long, Washington has treated offensive cyber operations as inherently escalatory — as if responding to a cyber intrusion carried the same risk as nuclear war. The result is a dangerous pattern: we absorb attack after attack, issue warnings about "norms," and add a modest sanction or two. Meanwhile, the People's Republic of China (PRC), Russia, Iran, and North Korea continue to infiltrate our critical infrastructure, steal our intellectual property, and pre-position malware inside our civilian systems — all with increasing confidence that there will be no real cost.

That restraint was meant to prevent escalation. In practice, it has invited it.

The following is a small fraction of the persistent and escalating campaign of cyber aggression directed against the United States.

We have watched as PRC-linked actors conducted the Salt Typhoon campaign, making deep, strategic infiltrations into multiple major American telecommunications providers, including AT&T, Verizon, and T-Mobile.

We have witnessed the systematic theft of our citizens' most private data:

- The compromise of Anthem impacted 79 million records—including Social Security numbers and medical IDs.

- We have seen the mass exfiltration of personal data from Marriott affect 383 million guests, including passport numbers.
- We have seen 145 million Americans—nearly half the country—have their financial identities stolen in the Equifax breach, an act for which members of the Chinese Military were directly indicted.
- We have seen 22 million records exfiltrated from the Office of Personnel Management, including the highly sensitive SF-86 security clearance files of our federal workforce. It included the Social Security numbers, fingerprints, and the most intimate background details of current, former, and prospective federal employees, contractors, and their families. By harvesting this data, the PRC has gained a permanent counterintelligence roadmap to the people who operate, protect, and lead this country.

Additionally, PRC actors have moved beyond espionage and begun embedding themselves within our critical infrastructure.

Through the campaign known as Volt Typhoon, PRC-linked actors have burrowed into the networks of U.S. water, power, and transit systems. According to public government reporting, this activity reflects deliberate pre-positioning to hold hostage our American cities and communities, and enable disruption during a future crisis or conflict.

The PRC is not alone. The 2014 Sony Pictures hack—conducted by North Korean actors—was not about theft alone. It was designed to destroy systems, disrupt operations, and impose real economic damage on a U.S. company.

These are no longer potential risks.

Our adversaries have learned that the marginal cost of doing more is low. Every time we respond to aggression with speeches instead of real consequences, we send a clear signal: keep climbing. Over time, that becomes a perverse incentive — one that rewards exactly the behavior we want to stop.

The cyber domain doesn't behave like the Cold War's nuclear world. Escalation is not automatic — which means policymakers have more room to act than their instincts suggest. We don't have to choose between doing nothing and doing something reckless. We can act proportionally, preemptively, and persistently.

Last year, National Cyber Director Sean Cairncross was correct in saying that the US needs to "shift the burden of risk in cyberspace from Americans to them." Director Cairncross recognizes that deterrence in cyberspace requires the credible, routine use of offensive power — not as a last resort, but as a standing expectation. Our adversaries are not deterred by words; they are deterred by disruption.

And the most effective time to disrupt an adversary is before their campaign becomes a headline. Preemptive operations — when executed responsibly — can deny access, degrade infrastructure, and raise the attacker's cost curve. They force our enemies to rebuild, defend, and think twice.

In the physical world, we would never allow a terrorist to walk across our borders, establish a terrorist cell in plain sight, and wait to stop them only at the moment they reach for the detonator. We don't wait for the trigger to be pulled or the button to be pressed on a bomb. We stop them well before they ever reach their target. Afterwards, our military, intelligence community, and law enforcement are praised for their ability to identify hostile infrastructure being built for the purpose of attacking America.

Cyberspace should be no different. We currently possess the technical ability to see the digital infrastructure of our enemies being constructed in the shadows of our networks. We can see the networking established with the intention to paralyze us. Yet, under our current passive doctrine, we are forced to watch and wait.

We need a policy of deterrence where we disrupt the threat at its origin, not at our doorstep. We can leverage the innovation of the private sector to dismantle these threats before they can be activated. If we can foresee an attack aimed at an American city or town, a Fortune 500 company or a federal agency, a state or local municipality, our duty is clear: we have the moral and national security obligation to neutralize the threat.

At Twenty, we partner closely with the United States Government to develop and deploy these capabilities at scale. We're helping to deliver exactly what deterrence now requires: speed, agility, and credible offensive power.

But this is not just about technology — it's about mindset. For years, we substituted process for power. We talked about responsible behavior, issued indictments that foreign operatives will never face, and redrew red lines every time they were crossed. That approach has failed not because America lacks cyber talent, but because we have been paralyzed by outdated theories of escalation.

To compete, we must build a new habit—responding. Every serious campaign against the United States must produce real, visible consequences.

Congress has a critical role to play by demanding measurable accountability. On a classified basis, Congress should require answers to the following questions: How quickly and how often were preemptive or proactive offensive cyber actions authorized to disrupt, deny, or degrade adversary operations? Did those actions reduce adversary persistence? And were hostile campaigns forced to degrade or rebuild?

These are the questions that should define cyber deterrence in the 21st century.

Technology will play a decisive role in this transformation — especially Artificial Intelligence. AI-enabled systems are already reshaping cyber operations, from accelerating target analysis to automating detection of vulnerabilities. At Twenty, we are developing AI-driven cyber tools that can operate securely within classified environments, multiply human capability by orders of magnitude, and do so responsibly, with human oversight.

Last year, Congress authorized one billion dollars for offensive cyber programs in H.R. 1. This was an important step, but only a down payment. We cannot treat it as a box checked. These funds must go toward future-focused technology — not legacy systems — and AI must be a central part of that investment. And, Congress should condition future offensive cyber funding on demonstrable improvements in speed, scale, and mission impact—favoring systems built for rapid, persistent cyber operations, not legacy platforms designed for episodic, one-off missions.

Ultimately, no single entity — not government, not industry — can meet this challenge alone. Our adversaries coordinate across government and private lines. We must do the same. The White House is right to emphasize public-private collaboration as a cornerstone of cyber deterrence. The United States has the talent, the innovation, and the moral clarity to lead in this new era — but leadership requires urgency, and it requires partnership.

At Twenty, we are proud to help make that possible — ensuring that America's cyber capabilities remain powerful, disciplined, and aligned with democratic values.

Thank you for the opportunity to testify. I look forward to your questions.