January 31, 2024

Testimony of Harry Coker, Jr.

National Cyber Director

Executive Office of the President

11:00 AM EST

United States House of Representatives

Select Committee on

Strategic Competition Between the U.S. and the Chinese Communist Party

Hearing on

“The CCP Cyber Threat to the American Homeland and National Security”

Chairman Gallagher, Ranking Member Krishnamoorthi, and distinguished Members of the select committee, thank you for holding this important hearing to highlight the risks that advanced persistent threat actors, associated with the People's Republic of China (PRC), pose to our nation and our allies and partners around the globe.

I am pleased to testify before you today. The work of the select committee is important, and I look forward to speaking to you about the bold vision this Administration has laid out in the National Cybersecurity Strategy (NCS), published less than one year ago.

I am honored to lead the Office of the National Cyber Director (ONCD) in the Executive Office of the President. ONCD, now in its third year, advises the President on cybersecurity policy and strategy related to the coordination of programs and policies intended to improve the cybersecurity posture of the United States. ONCD also leads the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy.

Coordination and collaboration are central to our ethos; cybersecurity requires a team effort and I am proud to be before you today with a few of ONCD's closest federal partners in creating the conditions for more defensible and resilient national critical infrastructure – Director Easterly, Director Wray and General Nakasone. Our organizations work together on a daily, and sometimes hourly, basis to protect the nation. I am very grateful for their partnership and also that of our many partner defenders in industry who own and operate the infrastructure so many of our fellow Americans depend on for critical services every day.

THREAT

This hearing is timely, given the significant threats we face in cyberspace, including from the PRC. We continue to see significant nation-state cyber espionage operations targeting government and private sector information systems. And the growing exploitation of Americans' sensitive data and improper use of surveillance technology, including commercial spyware, threatens the U.S. technology ecosystem. After decreasing in 2022, ransomware and related extortion schemes are on the rise again.

The threat under discussion today, though, is of a different nature. Our Intelligence Community has noted that a PRC threat actor is pre-positioning itself on U.S. critical infrastructure systems to potentially conduct disruptive and potentially destructive attacks in the event of a conflict. The threat PRC-sponsored cyber actor, "Volt Typhoon," as it has been named by a private sector partner, has conducted cyber operations focused not on financial gain, espionage, or understanding state secrets, but on developing deep access into critical infrastructure networks to put them at risk. If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations, leveraging accesses like those developed by Volt Typhoon, against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, interfering with the deployment of U.S. forces, and challenging our ability to project power in the region. Such a strike could also impact the American public and the services they rely on every day.

The discovery of Volt Typhoon activity on U.S. critical infrastructure is a clear warning to policymakers that the PRC is taking operational steps to prepare for such a conflict. Pre-positioning for disruptive or destructive operations, in line with the People Liberation Army's doctrinal approach to cyberspace, is the objective of Volt Typhoon.

Interagency partners at the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and United States Cyber Command (USCYBERCOM) worked together – and, vitally, with partners in the private sector – to identify signs of Volt Typhoon activity and share them publicly so that the broader cybersecurity community can take appropriate actions to protect targeted systems. This collaboration has been fundamental to fully understanding the scope of Volt Typhoon activity. It is every bit as fundamental to the work that remains to counter this particular PRC actor and others who intend to hold our critical infrastructure at risk.

THE PRESIDENT'S NATIONAL CYBERSECURITY STRATEGY

President Biden issued the National Cybersecurity Strategy last year. It highlights the President's bold vision for a prosperous, connected future and calls for us to build that future on a foundation of deep and enduring collaboration among stakeholders in the digital ecosystem.

The President also calls for two fundamental shifts in how we approach cybersecurity:

- First, we must "rebalance the responsibility to defend cyberspace." Today, end users of technology – be they individuals, small businesses, or critical infrastructure owners and operators – bear too much of the responsibility for keeping our nation secure. A system that can be brought down by an errant click on a phishing email is too brittle, and our adversaries will find our weaknesses and exploit them. Instead, we need to expect more of the most capable actors in cyberspace, including the government.
- Second, we must "realign incentives to favor long-term investments." Our digital infrastructure is vulnerable; we must build future systems to be more inherently defensible and resilient. Doing so means ensuring that market forces and public programs alike reward security and resilience.

Both of these shifts derive from an underlying strategic imperative: to seize the initiative from our adversaries. When we let threat actors define our objectives and are simply reactive, we are not advancing our vision for cyberspace, we are living in theirs. Seizing the initiative can mean persistently engaging adversaries, but it also can mean embracing secure by design principles that make it more difficult to carry out a successful operation.

ONCD is responsible for overseeing implementation of the Strategy. Last July, we publicly released an Implementation Plan highlighting 69 high-impact initiatives that will help achieve the President's vision. We are in the process of completing our first annual update of the plan, which we will continue to refine in light of evolving threats, emerging technologies, and feedback from our partners in the private sector; civil society; state, local, tribal, and territorial governments, and of course Congress.

Several of the Strategy's core objectives – and related implementation initiatives – relate to protecting our critical infrastructure from threat actors associated with the PRC and tipping the strategic initiative in our favor.

DEFEND CRITICAL INFRASTRUCTURE

The first pillar of the Strategy is simple in concept if daunting in scope: "Defend critical infrastructure." As we can see from PRC targeting, critical infrastructure systems are terrain we have to defend, and critical infrastructure owners and operators – the majority of whom are private entities, not governments – are on the front lines.

Part of our success, then, will come from scaling public-private collaboration. In the Implementation Plan, this manifests as, for example, CISA's work to drive the development and adoption of software and hardware that is secure-by-design and secure-by-default by identifying barriers to adoption and marshaling collective action to overcome them.

As the Implementation Plan calls for, we must also empower our sector risk management agencies (SRMAs) by providing them necessary support from CISA, which has unique responsibilities to coordinate cross-sector risk mitigation. ONCD and the Office of Management and Budget issued joint budgetary guidance last summer identifying for agencies key funding priorities, including priorities for SRMA activities. As key interlocutors with their sectors, SRMAs are lynchpins to any effort to scale collaboration.

We must also establish comprehensive and consistent minimum cybersecurity requirements for our critical infrastructure to support national security, economic security and public safety. Sharing situational awareness of PRC threat actors – which itself is an objective of the Strategy – is necessary, but not sufficient to meet the magnitude of the threat posed by the PRC and other malicious actors. When it comes to matters of national security, there is a clear need for mandatory cybersecurity requirements to both mitigate risk and to level the playing field to ensure that companies that do make investments in cybersecurity are not disadvantaged in the marketplace. Effective regulations, developed as part of a collaborative process involving regulators, industry, and other affected parties, can produce regulatory requirements that are operationally and commercially viable and that minimize the cost and burden of compliance, while significantly advancing cybersecurity. We have seen this strategic direction put into practice at the Transportation Security Administration, which has, in response to significant unmitigated risks, issued several Security Directives that put in additional cybersecurity requirements across the transportation sector, including for pipelines, rail, and aviation.

I am proud that ONCD is leading the Administration's efforts on cybersecurity regulatory harmonization. As we have seen in the more than 80 responses to our recent request for information on this topic, there are significant strides we all can make to reduce the compliance burden on companies while raising the baseline security posture.

Beyond scaling collaborative mechanisms and setting clear, harmonized cybersecurity requirements, the government must also be a good partner when an incident has occurred and federal assistance is required. To that end, and in accordance with the Implementation Plan, CISA, in coordination with ONCD and many other departments and agencies, has begun work to update the National Cyber Incident Response Plan. CISA, as the national lead for asset response, will work with interagency partners including the FBI, the lead for threat response, to include clear guidance to external partners on the roles and capabilities of federal agencies in incident response and recovery.

Taken together, these initiatives touch the contours of the Administration's significant scope of work to defend critical infrastructure from cyber threats. All of them are predicated on the partnership model that remains foundational to our success, and all are driven by the strategic imperative epitomized by threat actors like Volt Typhoon – that our critical infrastructure is already being infiltrated with a view towards disruption or destruction.

INVESTING IN THE FUTURE

Even as we shore up our defenses, we must also look to change the dynamics in cyberspace to favor defenders. That starts with our people.

In July 2023, ONCD released the National Cyber Workforce and Education Strategy (NCWES). Faced with over half a million open jobs in cyber fields, it is vital that we invest in workforce programs, from apprenticeships to skills-based hiring initiatives, to help address the immediate need that spans both government and private sector. But we must also do more to improve the pipeline of talent, expanding opportunities for all citizens to learn digital skills and opening these good-paying careers to all segments of society, including those who have never seen themselves in cyber. Implementing the NCWES will require us to build regional ecosystems across the country where industry, academia, and government come together to develop the workforce of the future. It will also necessitate the teaching of cyber skills across academic disciplines, different industrial sectors, and those in non-technical job functions.

Through programs funded by the Bipartisan Infrastructure Law, the Inflation Reduction Act, and the CHIPS and Science Act, the United States is making once-in-a-generation investments in our infrastructure and the digital ecosystem that supports it. The Administration is committed to making investments in a manner that increases our collective systemic resilience, which means designing, developing, fielding, and maintaining projects with cybersecurity and all-hazard resilience in mind. Whether it's through projects supporting defense critical infrastructure – those infrastructure assets vital to the operations, deployment, and mission assurance of our military – or advance chip fabrication facilities, building cybersecurity in from the outset protects our national interests and is much easier to do than trying to bolt it on after a new system is deployed.

These kinds of initiatives – retooling educational pipelines, building the infrastructure for the next generation, even accelerating modernization of federal information systems – are bold, but necessarily so. After all, the strategies employed by threat actors, particularly the PRC, envision cyberspace operations as important elements to the success of joint operations.

CLOSING

Improving the cybersecurity posture and resilience of critical infrastructure is a key pillar of the President's National Cybersecurity Strategy. In conjunction with our other work to disrupt and dismantle threat actors; shape market forces to drive security and resilience; invest in a resilient future; and forge international partnerships to pursue shared goals, we are making progress to achieve the bold vision the President set out for the country.

But we will not achieve that vision – and take back the initiative from PRC threat actors – without the foundational partnerships we rely on, including with Congress. Further strengthening those partnerships is a key priority of mine and of the Administration.

Cybersecurity requires unity of effort. Thankfully, our U.S. team has broad and deep partnerships comprising people from all levels of government and industry working together to build a defensible, resilient digital ecosystem.

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