

Testimony of

Steven M. Kelly
Chief Trust Officer
Institute for Security and Technology

before the Committee on Oversight and Accountability

Subcommittee on Cybersecurity, Information Technology,
and Government Innovation

U.S. House of Representatives

on

Red Alert: Countering the Cyberthreat from China

May 15, 2024

Chairwoman Mace, Ranking Member Connolly, distinguished members of the subcommittee, thank you for the opportunity to appear before you today to address the threat to our nation's critical infrastructure posed by cyberattacks from the People's Republic of China (PRC). My name is Steve Kelly and I serve as the Chief Trust Officer at the Institute for Security and Technology. IST is a 501(c)(3) critical action think tank that unites technology and policy leaders to create actionable solutions to emerging security threats.

Prior to joining IST, I served as a Special Agent in the Federal Bureau of Investigation's (FBI's) cyber program for over 21 years, and during that time twice served on joint duty assignments to the National Security Council (NSC) staff in the cybersecurity directorate. From 2013 to 2015, I served as Director for Cybersecurity Policy and focused on cyber incident management, insider threat, and aspects of federal agency cybersecurity. I served as the process facilitator and principal author of Presidential Policy Directive 41 on *United States Cyber Incident Coordination* which set policy for government-wide responses to nationally significant cyber incidents. I returned to the NSC's cybersecurity directorate in mid-2022 to serve as Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology, reporting to Deputy National Security Advisor Anne Neuberger and having responsibility for cyber defense, incident management, and critical infrastructure protection.

While I retired from the FBI nearly a year ago, my commitment to our nation's national security remains my highest professional priority and so I joined a think tank which focuses on these very issues. I will present my testimony along three themes: (1) managing exposure and dependencies; (2) protecting the homeland; and (3) partnering for success.

Managing exposure and dependencies

Both the current and previous administrations have been explicit about the threats that the PRC poses to the United States, our interests, and allies—as have many members of this subcommittee. Some of the ways the PRC and the Chinese Communist Party manifest those threats are in the cyber domain. My grave concern is rooted both in the PRC's illiberal global agenda and the means by which it seeks to realize that agenda, including through their compromised technology exports bearing subsidized low pricing and financing terms.

This follows at least two decades of China's "rob, replicate, and replace" strategy—as described by former Assistant Attorney General John Demers¹—which allowed Chinese firms to benefit from stolen American innovation, begin manufacturing identical products at lower cost, and put the victimized firm out of business. Over time and across numerous research and development areas, this strategy—enabled by state-sponsored economic espionage on a scale never before seen—has allowed the PRC's technology industry to rapidly catch up and in some cases surpass the United States and allied nations.

¹ Assistant Attorney General John C. Demers Remarks for Press Conference on United States V Li, et al., <https://www.justice.gov/opa/speech/assistant-attorney-general-john-c-demers-remarks-press-conference-united-states-v-li-et>

Chinese technology products, both inside the PRC and for export, prioritize state-level interests over users' security and privacy, exposing users to government surveillance; serving as a vector for cyber operations; and, in the event of contingency, potentially enabling denial and disruption actions. The FCC in 2020 designated Chinese technology firms Huawei and ZTE as threats to U.S. national security² and provided funds to “rip and replace” existing Huawei and ZTE equipment from U.S. telecommunications networks. Identifying and replacing Chinese technology from U.S. and allied telecommunications networks remains a significant challenge to this day, in part because all of the “rip and replace” funds have been exhausted.³ Even when briefed on the risks, developing economies often find the immediate need for economic development more important than the potential longer-term foreign intelligence risk.

Indeed, no global competitor threatens democratic rules, norms, and American technological superiority more than the PRC, which creates technologies and tech policies that facilitate genocide domestically and perpetuate authoritarian interests abroad.

Fuel and protect the cycle of innovation

One of the core functions of any government is to protect private property, and nowhere is this more needed than with regard to the PRC government's decades-long industrial-scale expropriation of U.S. intellectual property. Where justice through civil or criminal remedies is not possible—or preferred, for example, when public disclosure would jeopardize U.S. Intelligence Community operations—the U.S. should employ other tools of statecraft. This includes export controls, visa bans, sanctions such as Treasury's recent designation of the Ministry of State Security front company Wuhan Xiaoruzhi Science and Technology Company,⁴ and diplomatic actions such as the U.S.-ordered closure of the PRC's consulate in Houston.⁵ These steps, in concert with similar actions by our allies and partners, contribute to preserving our democracy and innovation economy.

Also, Silicon Valley and innovation ecosystems across the country are experiencing a resurgence of interest in this topic and stakeholders in the technology ecosystem are taking action. For example, a group of leading U.S. cyber and advanced technology investors recently announced their voluntary investment principles and commitments to put trust, safety, and

² “FCC Designates Huawei and ZTE as National Security Threats”, *Federal Communications Commission*, January 30, 2020, <https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats>

³ “Chairwoman Updates Congress on 'Rip and Replace' Funding Shortfall”, *Federal Communications Commission*, <https://www.fcc.gov/document/chairwoman-updates-congress-rip-and-replace-funding-shortfall>

⁴ “Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure”, *U.S. Department of the Treasury*, March 25, 2024, <https://home.treasury.gov/news/press-releases/jy2205>

⁵ “Briefing With Senior U.S. Government Officials On the Closure of the Chinese Consulate in Houston, Texas”, U.S. Department of State, July 24, 2020, <https://2017-2021.state.gov/briefing-with-senior-u-s-government-officials-on-the-closure-of-the-chinese-consulate-in-houston-texas/>

security at the center of the technological innovation they are funding to “ensure, to the maximum extent possible, that the technologies cannot be used against our democracy and our people.”⁶ Another leading venture capital firm announced its American Dynamism⁷ effort and an array of both incumbent and insurgent investors and founders are driving a new and powerful defense tech-focused movement.

Assist trusted technology to be globally competitive

While it has been a long time coming, many throughout the world have come to recognize the risks that often accompany lower-cost Chinese products and are procuring technology from more trustworthy sources, even at a price premium. I played a small part in planning and launching the *U.S. Cyber Trust Mark*, a voluntary security labeling program for consumer Internet-of-Things (IoT) devices adopted in March by the Federal Communications Commission⁸ that will “help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards.” Other countries, including Singapore,⁹ Finland, and Germany have launched their own cybersecurity labeling programs, thus it is important that the United States step in with its own approach to influence international standards and reciprocity.

As an extension of this effort, the National Institute for Standards and Technology is undertaking an effort to “define cybersecurity requirements for consumer-grade routers—a higher-risk type of product that, if compromised, can be used to eavesdrop, steal passwords, and attack other devices and high value networks.”¹⁰ (*More on routers below.*) Even more compelling, given the PRC cyber threat to critical infrastructure discussed below, the Department of Energy committed to research and develop cybersecurity labeling for energy products.¹¹

Industry-led efforts by the Consumer Technology Association and Connectivity Standards Alliance align with the FCC’s labeling program, as many manufacturers in the U.S. and allied countries are eager to participate. While the FCC has already taken first steps under § 302 of

⁶ “Investment Principles and Commitments on Trust, Safety, and Security”, *Paladin Capital*, March 7, 2024, <https://www.paladincapgroup.com/investment-principles-and-commitments/>

⁷ “American Dynamism”, *Andreessen Horowitz*, <https://a16z.com/american-dynamism/>

⁸ “FCC Creates Voluntary Cybersecurity Labeling Program for Smart Products”, *Federal Communications Commission*, March 14, 2024, <https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf>

⁹ “Singapore’s Cybersecurity Labelling Scheme (CLS)”, *Cyber Security Agency of Singapore*, <https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme>

¹⁰ “Improving Consumer IoT Cybersecurity”, *National Institute of Standards and Technology*, <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity>

¹¹ “Biden-Harris Administration Launches New Effort to Advance Cyber Labeling and Security Transparency for Energy Products and Systems”, *U.S. Department of Energy*, <https://www.energy.gov/ceser/articles/biden-harris-administration-launches-new-effort-advance-cyber-labeling-and-security>

the Communications Act of 1934, I encourage Congress to ensure the program's future stability and success by specifically authorizing and funding it.

Safeguard American critical manufacturing

The dramatic shift of American manufacturing to the PRC accelerated following its acceptance into the World Trade Organization. However, the supply chain implications of this shift were not fully appreciated until 2020, when shortages in everything from personal protective equipment to semiconductor chips for cars became painfully obvious to even the casual observer. The CHIPS and Science Act of 2022 represents an American response to that situation, setting in motion the revitalization of domestic semiconductor fabrication and broader innovation across almost twenty categories of critical and emerging technologies.

While I believe it is typically preferable to allow the private sector to allocate capital and make its own business decisions, in light of the risks driven by the PRC's aggressive policies, the United States and our allies must maintain key industries for national security reasons, including semiconductor fabrication, core telecommunications equipment, novel energy development, rare earth mineral extraction, and vaccine and drug manufacturing.

Protecting the homeland

The Intelligence Community's 2024 Annual Threat Assessment (ATA) explained that PRC cyber operations were intended as pre-positioning on critical infrastructure for use during conflict to "impede U.S. decisionmaking, induce societal panic, and interfere with the deployment of U.S. forces."¹² This assessment is further supported by very similar warnings by CISA Director Jen Easterly in early 2023,¹³ the "Volt Typhoon" cybersecurity advisory in February,¹⁴ and FBI Director Chris Wray last month.¹⁵ To speak plainly, this means that the nation's experts on Chinese cyber programs have concluded that Beijing is preparing to use American infrastructure against us, or more specifically, the threat of infrastructure failure to deter the United States from taking action when the Chinese military tries to invade Taiwan. This assessment should inspire a new sense of urgency to remove the PRC's leverage by consistently counteracting and publicly exposing their cyber intrusion means—such as FBI's operation to cleanse hundreds of

¹² "Annual Threat Assessment of the U.S. Intelligence Community", *Office of the Director of National Intelligence*, February 5, 2024, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>

¹³ "CISA Director Easterly Remarks at Carnegie Mellon University", *Cybersecurity and Infrastructure Security Agency*, February 27, 2023, <https://www.cisa.gov/securebydesign/dir-easterly-remarks-carnegie-mellon-university>

¹⁴ "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure", *Cybersecurity and Infrastructure Security Agency*, February 7, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

¹⁵ "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says", *Federal Bureau of Investigation*, April 18, 2024, <https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-in>

small office/home office routers hijacked by PRC state-sponsored hackers¹⁶—and by hardening U.S. critical infrastructure functions against disruption.

Given numerous cyber attacks impacting critical infrastructure services over the past several years, including the ransomware attacks on Colonial Pipeline, JBS Foods, and an untold number of hospital systems—to include Ascension health system just last week—we are clearly not doing enough to manage cyber risk to essential public services. While ransomware is not the focus of this hearing, it is instructive of the range of real-world impacts that cyber operations can deliver. IST has co-chaired a Ransomware Task Force since 2021 that has detailed how deeply susceptible many critical sectors—including healthcare, manufacturing, and government services—remain to fairly straightforward, unsophisticated ransomware attacks.¹⁷ If criminal gangs in Russia can achieve these effects, the People’s Liberation Army most certainly can too when called upon.

The very term critical infrastructure connotes prioritization—what is “critical” and what is not. To inform the protection of that which may be at risk in the event of an escalation with China, I would like to offer my suggested approach, phrased as a question: “What are the services that everything else relies upon?” My answer is (1) electricity, (2) water, (3) communications, and (4) transportation, which tracks closely with a narrow list of key sectors identified in a recent Defense Department statement on critical infrastructure security and resilience.¹⁸ For example, water cannot be purified and distributed without electricity. In many cases, power plants require municipal water for cooling. Food cannot be delivered to population centers without transportation. Hospitals cannot function for long without all four of these. Frankly, modern society would quickly unravel without these four.

Through its National Cybersecurity Strategy, the Biden Administration called for establishing minimum cybersecurity requirements for critical infrastructure through regulation, or where such authority does not exist, to seek it. The President’s recently announced National Security Memorandum on *Critical Infrastructure Security and Resilience*¹⁹—a long-awaited refresh of President Obama’s directive bearing the same name—also calls for critical infrastructure entities

¹⁶ “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure”, *U.S. Department of Justice*, January 31, 2024, <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>

¹⁷ “Ransomware Task Force, Doubling Down: April 2024 Progress Report”, *Institute for Security and Technology*, April 24, 2024, <https://securityandtechnology.org/wp-content/uploads/2024/04/April-2024-RTF-Progress-Report-Doubling-Down.pdf>.

¹⁸ “DOD Support to National Security Memorandum 22”, *U.S. Department of Defense*, May 7, 2024, <https://www.defense.gov/News/Releases/Release/Article/3766979/dod-support-to-national-security-memorandum-22/>

¹⁹ National Security Memorandum 22 on “Critical Infrastructure Security and Resilience”, *The White House*, April 30, 2024, <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>

to maintain a minimum cybersecurity posture under regulation. And where such authority to regulate is lacking, the memorandum instructs the relevant agency to submit a legislative proposal to gain such authority. Deputy National Security Advisor Anne Neuberger has been quite vocal on this point as she pressed for setting minimum cybersecurity requirements through a pragmatic “sector-by-sector” approach, cognizant that the patchwork of authorities and gaps precluded a uniform approach across all sectors.

While federal regulations are not appropriate or desired in all circumstances, I believe that ensuring the security and resilience of functions essential to national security, economic security, or public health and safety warrants a regulatory approach—these are essential public services, and the American people can rightfully expect the government to take steps to ensure their resilience. In order to minimize the regulatory burden, the memorandum calls for maximum cross-sector harmonization of requirements, leveraging consensus-based standards and best practices.

To date, efforts to establish such minimum requirements have met with mixed results, leaving some sectors without such mandates. One example is the information technology (IT) sector, largely unregulated, but for President Trump’s 2021 executive order to address PRC misuse of U.S.-based Infrastructure as a Service (IaaS) products,²⁰ which is now moving forward under Department of Commerce rulemaking.²¹ The IT sector includes cloud services (which includes IaaS) and major technology platforms that nearly all Americans rely upon daily. For example, few Americans today have a traditional “landline” telephone, and instead rely on their smartphone and home broadband Internet connection—with Wi-Fi router—to talk, text, and video chat with those next door and around the world. These services rely on the cloud and involve software-defined networks, making it increasingly difficult to tell the difference between a legacy telecommunications company, which is heavily regulated, and a cloud service provider, which is not. There is no doubt in my mind that communications is a national critical function which must be resilient to a variety of hazards.

Another powerful example involves hospitals. Cybersecurity firm Emsisoft earlier this year reported that 46 hospital systems were impacted by ransomware attacks in 2023—up significantly from the year before²² and often resulting in inaccessible medical records, canceled procedures, and ambulance diversions to other hospitals. A recent article published in the health, medicine, and life sciences media outlet *STAT* described these impacts and claims

²⁰ E.O. 13984 on “Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities”, *The White House*, January 25, 2021, <https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious>

²¹ Proposed Rule on “Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities”, *U.S. Department of Commerce*, January 29, 2024, <https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious>

²² “The State of Ransomware in the U.S.: Report and Statistics”, *Emsisoft*, January 2, 2024, <https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/>

“cyberattacks interrupt care delivery and threaten patient safety” and estimated that ransomware attacks killed between 42 and 67 Medicare patients between 2016 and 2021.²³ And this year is off to another inauspicious start, with 18.7 percent of ransomware incidents in the first quarter reportedly targeting healthcare providers—making it, to date, the most frequently targeted sector.²⁴

Hospitals are primarily regulated in three areas: patient safety, patient privacy, and billing of services. The most relevant statute to hospital cybersecurity is the Healthcare Insurance Portability and Accountability Act (HIPAA), which addresses patient privacy, including in the context of data breach. However, I believe the provision of time-sensitive care—treating emergencies like heart attacks, strokes, and severe trauma—is the critical function in greatest need of protection. If I were a patient experiencing one of these issues, I would not be too concerned about the privacy of my data at that very moment, but much more so about whether the nearest trauma center is diverting patients due to a ransomware or state-sponsored cyber attack. I would encourage members to consider whether the Department of Health and Human Services’ authorities, as both the sector risk management agency and regulator, are focused on the right outcomes. I will also note that state health regulators can also take action to protect these vital services.

If establishing baseline requirements for critical infrastructure is to be achieved—which I think is warranted—Congress will inevitably need to create or clarify regulatory authorities for certain sectors. And each sector risk management agency and regulator must be commensurately resourced to have the personnel and expertise needed to carry out the task.

Partnering for success

The critical infrastructure facilities in need of protection are scattered throughout the nation, and it is difficult to meet their needs from Washington, DC. Fortunately, there are a variety of players across the federal enterprise who are able to engage at the local level. I suggest that Congress be creative in how these field forces are teamed to achieve critical mass and provide maximum value to critical infrastructure owners and operators and the American taxpayer.

I’ll start with the Cybersecurity and Infrastructure Security Agency’s (CISA’s) cybersecurity advisor (CSA) program, which places cybersecurity professionals across the country to assist critical infrastructure owners and operators and state, local, tribal, and territorial (SLTT) officials with advice, preparedness assessments, and a path to other CISA cyber services. However, this program is still quite new and often a large area may have only one such advisor. While I

²³ Neprash, Hannah; McGlave, Claire; Nikpay, Sayeh. “We tried to quantify how harmful hospital ransomware attacks are for patients. Here’s what we found”, *STAT*, November 17, 2023, <https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/>

²⁴ Siegel, Bill. “RaaS Devs Hurt Their Credibility by Cheating Affiliates in Q1 2024”, *Coveware: Ransomware Recovery First Responders*, April 17, 2024, <https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024>.

encourage Congress to resource sufficient advisors to cover the ground, what remains clear is the need for expanded and enhanced partnerships as force multipliers to ensure success.

Fortunately, CISA's field cyber advisors are not alone. Notably, the Federal Bureau of Investigation and United States Secret Service have cyber task forces in field offices across the country, which maintain relationships with key critical infrastructure entities in the local area, investigate cyber threats, notify victims and potential victims, and respond to cyber incidents. Emulating the successful nationwide Joint Terrorism Task Force (JTTF) program, there exists an incredible opportunity to team federal and SLTT personnel to undertake both proactive and reactive cybersecurity efforts.

I would be remiss if I neglected to discuss how military cyber units might fit into this model. National Guard cyber units acting under their respective Governor's authorities are well postured to partner with a local joint cyber task force. Through it, they can gain improved situational awareness to the threats affecting their areas of responsibility and, particularly with respect to municipally owned critical infrastructure, could be deployed to conduct proactive vulnerability assessments and even reactive incident response support.

Given the topic of this hearing and the IC's assessment discussed above, I think it is worth considering what authorities might exist, or be needed, for active duty Cyber Protection Teams (CPTs) under Title 10 to provide assistance or even protection to select civilian critical infrastructure facilities essential to the operation of key military installations—also referred to as Defense Critical Infrastructure. While this approach may not scale, I believe there are scenarios under which it would make sense and should be explored.

In conclusion, I want to thank the subcommittee for inviting me to participate in today's timely hearing. We value this opportunity to raise awareness about threats our nation faces. IST and other civil society organizations like it, with the support of philanthropic gifts, corporate contributions, and project-specific grants, are well-positioned to contribute to addressing them.

I look forward to your questions.

###