WRITTEN TESTIMONY of Patrick C. Miller

President & CEO, Ampyx Cyber

*before the*

U.S.-CHINA ECONOMIC and SECURITY REVIEW COMMISSION

*concerning*

"*China's Domestic Energy Challenges and Its Growing Influence over International Energy Markets*"

APRIL 24, 2025

Co-Chairs Commissioner Carte Goodwin and Commissioner Hal Brands, and members of the committee, thank you for the opportunity to testify on a topic critical to our nation's security. My name is Patrick Miller, and I am the President and CEO of Ampyx Cyber, a consulting firm specializing in cybersecurity for critical infrastructure, particularly energy systems. For more than 25 years, I have worked directly with every size and function of electric utility, as well as federal and state agencies, Information Sharing and Analysis Centers, and industrial technology hardware and software manufacturers to assess and mitigate cyber risk. I was one of the original contributors to the North American Electric Reliability Corporation Critical Infrastructure Protection, or NERC CIP, security regulations for the electric power sector. Further, I was the first auditor with delegated federal authority to monitor and enforce the NERC CIP regulations in the country. Most of my professional career has been dedicated to protecting the critical energy sector. I appreciate the opportunity to provide testimony on the threats posed by Chinese energy policy and technology practices. My testimony is based not only on public intelligence and open-source threat reporting, but also on direct field observations during my career.

**Background**

The cybersecurity of the United States power grid has emerged as one of the most urgent national security issues of the 21st century. As the grid becomes increasingly digitized and interconnected, it is also becoming more vulnerable to sophisticated cyberattacks—particularly those orchestrated by state-sponsored actors. Among these, Chinese state sponsored actors and criminals stand out as the most persistent and capable adversaries, with a clear strategic interest in targeting US critical infrastructure. Over the past several years, a growing body of evidence from federal agencies, congressional testimony, industry reports, and investigative journalism has revealed the scale, seriousness, and urgency of this threat.

China's cyber operations against the US power grid are not isolated acts of espionage or theft; rather, they are part of a broader campaign to pre-position disruptive capabilities within American networked infrastructure. The goal appears to be to create options for China to sow chaos and impede US military responses during a future crisis, especially one involving Taiwan. Just last year, Former FBI Director Christopher Wray warned Congress that these actors are actively "positioning on American infrastructure in preparation to wreak havoc and cause real world harm to American citizens and communities if and when China decides the time is right to strike"[1] and that Beijing's resources dedicated to cyber warfare was bigger "than every other major nation combined." [2] The US House Committee on Homeland Security has documented more than 60 instances of Chinese espionage on US soil in recent years, spanning cyber intrusions, intellectual property theft, and even transnational repression.[3]

The scope of China's targeting is vast. While the electric grid is a documented target, Chinese cyber actors have also probed and penetrated water treatment plants, oil and natural gas pipelines, transportation systems, and telecommunications networks. These attacks are not limited to the largest utilities; smaller organizations with limited cybersecurity resources are often compromised first, serving as steppingstones to larger and more critical targets.[4]

One of the most active and concerning groups in this space is Volt Typhoon. This Chinese state-sponsored advanced persistent threat (APT) group has been active since at least 2021, focusing on cyber espionage and pre-positioning for potential disruptive attacks. Volt Typhoon is particularly notable for its use of "living off the land" (LOTL) techniques, which involve leveraging tools and applications which are not introduced by the attacker, but are legitimate components of the operating system, commonly used for administration, automation, or troubleshooting. By using these native tools, Volt Typhoon is able to blend in with normal or expected activity, making detection much more difficult and allowing the group to maintain persistent access for extended periods.[5]

---

[1] Robert Walton, China-linked hackers primed to attack US critical infrastructure, Utility Dive (Jan. 31, 2024), https://www.utilitydive.com/news/fbi-china-hackers-us-critical-infrastructure/706423/

[2] Gareth Evans, FBI says Chinese state hacker group targeted US infrastructure, BBC News (Jan. 31, 2024), https://www.bbc.com/news/world-asia-68163172

[3] U.S. House Comm. on Homeland Sec., Threat Snapshot: CCP Espionage, Repression on U.S. Soil is Growing (Feb. 12, 2025), https://homeland.house.gov/2025/02/12/threat-snapshot-ccp-espionage-repression-on-us-soil-is-growing/

[4] Cybersecurity and Infrastructure Security Agency, National Security Agency & Federal Bureau of Investigation, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, CISA Alert AA24-038A (2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[5] Cybersecurity & Infrastructure Security Agency, Nat'l Security Agency & Fed. Bureau of Investigation, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Joint Cybersecurity Advisory AA24-038A (Feb. 7, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

A case that illustrates the sophistication and stealth of Volt Typhoon's operations involved the Littleton Electric Light and Water Departments (LELWD) in Massachusetts. The group infiltrated the utility's operational technology (OT) systems and, although operations were not disrupted, they remained embedded in the environment undetected for over 300 days, collecting data that could potentially facilitate future disruptive attacks. The breach was only discovered after the FBI alerted the utility, highlighting the importance of federal-private sector collaboration and the challenges of detecting advanced adversaries.[6]

The vulnerabilities exploited by Chinese actors are often rooted in the long operational lifespan of grid devices and the availability of outdated equipment. Many components in the US power grid were designed and installed decades ago, before modern cybersecurity standards were established. Some devices stay in service for decades and still run outdated software or systems that were never designed with cybersecurity in mind. Attackers exploit these weaknesses, especially in devices that are difficult or costly to upgrade or replace. The growing use of Chinese-manufactured components in the grid supply chain further complicates the risk landscape, raising concerns about potential backdoors or hidden vulnerabilities.[7,8]

In response to these threats, federal agencies have issued a series of urgent advisories and guidance documents. The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) have published joint advisories warning of the tactics, techniques, and procedures (TTPs) used by Volt Typhoon and other Chinese threat actors. These advisories urge critical infrastructure organizations to implement robust network segmentation, monitor for anomalous use of legitimate admin tools, and share incident information promptly with federal authorities. Congressional testimony has emphasized the need for improved information sharing between the private sector and government,[9] as well as the importance of modernizing legacy infrastructure to reduce vulnerabilities.[10]

International collaboration has also played a key role in the US response. The United States has worked closely with allies to share threat intelligence and best practices for defending critical

---

[6] Michael Kan, Chinese Hackers Sat Undetected in Small Massachusetts Power Utility for 300 Days, PCMag (Mar. 12, 2025), https://www.pcmag.com/news/chinese-hackers-sat-undetected-in-small-massachusetts-power-utility-for

[7] U.S. Dep't of Energy, DOE Leads Effort to Improve the Cybersecurity of Energy Supply Chains (June 18, 2024), https://www.energy.gov/articles/doe-leads-effort-improve-cybersecurity-energy-supply-chains

[8] Harry Krejsa, Sun Shield: How Clean Tech & America's Energy Expansion Can Stop Chinese Cyber Threats, Carnegie Mellon Inst. for Strategy & Tech. (Jan. 2025), https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html

[9] Helena Fu, Director, Office of Critical & Emerging Technology, U.S. Dep't of Energy, Testimony Before the S. Comm. on Energy & Nat. Res. (Sept. 12, 2024), https://www.energy.gov/sites/default/files/2024-09/SENR%20Hearing%20HF%20AI%20Testimony_Final.pdf

[10] Robert Walton, China-linked hackers primed to attack US critical infrastructure, Utility Dive (Feb. 1, 2024), https://www.utilitydive.com/news/fbi-china-hackers-us-critical-infrastructure/706423/

infrastructure.[11] This collective approach is essential, given the global nature of supply chains and the transnational reach of cyber adversaries.

Private sector and academic organizations have contributed valuable insights and recommendations. Cybersecurity firms have published technical analyses of Volt Typhoon's operations, underscoring the importance of foundational cyber defense capabilities and rapid incident response.[12] Academic white papers, such as the "Sun Shield" report from Carnegie Mellon University,[13] argue that the ongoing clean energy transition presents both risks and opportunities for grid cybersecurity. While the adoption of digitally-native, software-defined technologies can improve resilience, heavy dependence on Chinese-manufactured components introduces new supply chain vulnerabilities.

**Global Trends and Threat Evolution**

The cyber threat landscape targeting critical infrastructure has shifted dramatically over the past decade. Chinese state-aligned actors have moved from broad-spectrum cyber espionage campaigns to targeted pre-positioning within critical national infrastructure (CNI), indicating a strategic pivot from intelligence collection to the preparation of sabotage capabilities. This evolution aligns with China's broader doctrine of integrated warfare, in which cyber operations are used to shape the battlespace long before conventional conflict arises. This "access now, exploit later" strategy marks a dangerous escalation in China's global cyber posture.

Globally, countries such as Australia, Japan, the United Kingdom, and several NATO members have issued public warnings regarding increasing Chinese cyber intrusions into their energy, telecommunications, and transportation networks. The European Union Agency for Cybersecurity (ENISA) and the U.K. National Cyber Security Centre (NCSC) have both identified the PRC as a significant source of cyberattacks on infrastructure, often masked as supply chain compromises or remote service exploits.[14]

China's Belt and Road Initiative (BRI), particularly its Digital Silk Road component, has facilitated the global proliferation of potentially compromised infrastructure. By offering subsidized deals and attractive financing, Chinese state-linked firms such as Huawei and ZTE

---

[11] Cybersecurity and Infrastructure Security Agency, National Security Agency & Federal Bureau of Investigation, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, CISA Alert AA24-038A (2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[12] Mandiant, Volt Typhoon Brief (Jan. 9, 2024), https://static.carahsoft.com/concrete/files/1417/1198/7095/Mandiant-Volt-Typhoon-Brief-Public.pdf

[13] Harry Krejsa, Sun Shield: How Clean Tech & America's Energy Expansion Can Stop Chinese Cyber Threats, Carnegie Mellon Inst. for Strategy & Tech. (Jan. 2025), https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html

[14] Eur. Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023 (Oct. 19, 2023), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

have exported telecommunications systems, SCADA platforms, and digital control equipment to countries across Africa, Southeast Asia, Latin America, and Eastern Europe. These deployments often include bundled managed services, cloud platforms, and firmware update mechanisms controlled by PRC-affiliated vendors, thereby creating avenues for persistent access under the guise of legitimate operations. This strategy has raised significant concerns among international security experts regarding espionage risks, data sovereignty, and the potential for embedded surveillance capabilities within critical infrastructure.[15]

In parallel, Chinese hacking groups have continued to harvest large volumes of personal and organizational data from commercial breaches. The 2015 U.S. Office of Personnel Management (OPM) breach, the 2023 Microsoft email server breach, and the 2024 Salt Typhoon attack on major telecom firms illustrate an enduring interest in exploiting identity infrastructure and personal metadata as auxiliary targets. These datasets, among others available through criminal channels, can be aggregated and mined, then correlated with infrastructure operator credentials or leveraged for social engineering operations, reinforcing the strategic value of long-term surveillance.

Finally, the advent of generative artificial intelligence has accelerated both the speed and scale of potential cyber operations. Chinese cyber actors are now believed to be using AI to automate reconnaissance, exploit development, and social engineering campaigns at unprecedented scale. In testimony to Congress, senior intelligence officials have emphasized the risk that AI-enhanced intrusions will undermine the ability of defenders to detect and respond in real time.[16]

The combination of these trends paints a clear picture: the Chinese government is refining a full-spectrum, globally scalable cyber capability with the express purpose of undermining adversaries' infrastructure before, during, or even in lieu of conventional hostilities. Western nations must adapt by treating these digital threats with the same urgency and strategic foresight as kinetic threats, recognizing that infrastructure pre-positioning is not theoretical, but operationally underway.

**Espionage and Sabotage Susceptible Equipment**

---

[15] Council on Foreign Relations, Assessing China's Digital Silk Road Initiative, https://www.cfr.org/china-digital-silk-road/; 3GIMBALS, China’s Telecommunications Infiltration: A Growing Security Risk in Latin America, https://3gimbals.com/insights/chinas-telecommunications-infiltration-a-growing-security-risk-in-latin-america/

[16] Emma Stewart, Chief Power Grid Scientist, Idaho Nat'l Lab., Written Testimony Before the U.S. House Select Committee on the CCP, 118th Cong. (2024), https://democrats-selectcommitteeontheccp.house.gov/sites/evo-subsites/democrats-selectcommitteeontheccp.house.gov/files/evo-media-document/opening-statement-emma-stewart-final.pdf

The electric grid and broader energy infrastructure contain a range of components that are susceptible to exploitation for intelligence-gathering purposes. These include smart meters, supervisory control and data acquisition (SCADA) systems, remote terminal units (RTUs), energy management systems (EMS), intelligent electronic devices (IEDs), and other digital sensors and controllers that communicate across operational networks.

While traditional grid components such as transformers may not seem digitally sophisticated, many are now equipped with embedded digital control systems and auxiliary devices that collect operational data and relay it back to asset owners or service providers. For instance, load tap changers (LTCs), dissolved gas analysis (DGA) sensors, and digital relays have become standard for monitoring and optimizing equipment performance. If these digital subcomponents are compromised or covertly transmitting data, they may provide adversaries with operational insights about grid configuration, load characteristics, asset health, and control patterns.[17]

The risk is exacerbated when these devices are sourced from foreign entities with known affiliations to adversarial governments. Data exfiltration could be disguised as routine telemetry or system health reporting. Once collected, such information could be used to develop highly tailored attack plans, map out grid topology, or identify targets for disruption in a crisis scenario. Espionage at this level enables adversaries to understand not just what infrastructure exists, but how and when it operates—turning infrastructure visibility into operational leverage.[18]

These risks are not theoretical. Intelligence officials have testified to Congress that Chinese state-sponsored groups such as Volt Typhoon and Salt Typhoon are known to exfiltrate operational information to support broader strategic objectives, including pre-positioning and targeting of critical infrastructure.[19] In 2024, according to both the Wall Street Journal and Google Cloud's Mandiant unit, Chinese cyber actors gained access to SCADA networks across multiple sectors, including energy, using vulnerabilities in edge devices and misconfigured remote access tools.[20]

In addition to the risk of espionage, Chinese-manufactured components present credible risks of remote sabotage—particularly during periods of geopolitical crisis. The types of equipment most vulnerable to sabotage include devices with embedded software, remote access capabilities, firmware updaters, or connectivity to cloud management portals. This category spans from

---

[17] Federal Energy Regulatory Commission (FERC), *Cybersecurity of Electric Transmission Control Devices*, 2022, https://www.ferc.gov.

[18] Stewart, Emma, *Written Testimony Before the U.S. House Select Committee on the CCP*, March 5, 2025, https://democrats-selectcommitteeontheccp.house.gov/sites/evo-subsites/democrats-selectcommitteeontheccp.house.gov/files/evo-media-document/opening-statement-emma-stewart-final.pdf

[19] Ibid

[20] Volz, Dustin and Strohm, Chris. "In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks," *Wall Street Journal*, March 8, 2025, https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb; Gallagher, Sean. "China Acknowledges US Infrastructure Hacks in Leaked Cybersecurity Report," *WIRED*, March 8, 2025, https://www.wired.com/story/china-admits-hacking-us-infrastructure/

digital protective relays and programmable logic controllers (PLCs) to industrial firewalls, communications gateways, and battery energy storage systems (BESS).

Transformers, while traditionally seen as passive equipment, often include auxiliary systems that may have digital interfaces—especially load tap changers (LTCs), which regulate voltage output. Modern LTCs include motor drive units, relay logic, and control boards, which in some cases are network-connected or remotely configurable. A solution here could be only using manual control for critical transformers or engineering out the use of vulnerable components.

Battery energy storage systems are another concern. A 2022 study sponsored by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) found that over 90% of grid-scale BESS deployed in the U.S. contain critical components manufactured in China, including battery management systems (BMS), power conversion systems (PCS), and supervisory interfaces. These components are capable of firmware updates and telemetry reporting. If malicious firmware is pre-installed or remotely deployed, it could cause sudden outages, physical damage to energy assets, or even thermal runaway events in batteries.[21]

Sabotage risks are not limited to generation and storage. Substation automation systems, industrial routers, and remote terminal units—particularly those sourced from high-risk suppliers—can serve as pivot points to manipulate field devices or issue unauthorized control commands. Remote sabotage may not require sophisticated malware: it may simply involve leveraging a preconfigured access path, hard-coded credentials, or a dormant exploit awaiting activation.

U.S. officials and cybersecurity researchers have warned that Volt Typhoon and other Chinese groups have specifically sought to identify these "choke point" devices—small, often-overlooked components that can yield outsized control over grid operations. Once access is gained, even limited disruption can ripple across transmission networks, impair restoration efforts, or delay military deployments in a crisis.[22]

Reducing our dependence on foreign-manufactured grid components requires not only reshoring production capacity but also securing the upstream materials essential for that production Critical minerals are the foundational inputs for semiconductors and control boards—the essential components required to domestically manufacture transformers, inverters, battery management systems, and other core elements of grid infrastructure. Without secure and diversified access to

---

[21] Emma Stewart, Written Testimony Before the H. Select Comm. on the CCP, 118th Cong. (Mar. 5, 2025), https://democrats-selectcommitteeontheccp.house.gov/sites/evo-subsites/democrats-selectcommitteeontheccp.house.gov/files/evo-media-document/opening-statement-emma-stewart-final.pdf

[22] Robert Joyce, Testimony Before the H. Select Comm. on the CCP, 118th Cong. (Mar. 5, 2025), https://www.congress.gov/event/118th-congress/house-event/116479

these minerals, any effort to reshore the manufacturing of energy technologies will face severe constraints.

Mitigation of these risks requires an urgent shift from component-level testing to system-level risk modeling, with particular emphasis on country-of-origin sourcing, software assurance, and remote access pathways. Until the supply chain is more trusted and transparent, resilience must rely on active monitoring, strict segmentation, firmware verification, and the ability to operate in degraded modes without reliance on remote services.

**U.S. Reliance on Chinese Energy Equipment**

The United States' reliance on Chinese-manufactured energy equipment—particularly within critical infrastructure—presents a long-term strategic vulnerability. This dependency spans multiple layers of the electric power system, including grid components such as transformers, inverters, protective relays, industrial control devices, and energy storage systems. In many cases, these components are either wholly manufactured in the People's Republic of China (PRC), assembled from PRC-made subcomponents, or integrated with firmware and software developed by PRC-affiliated firms.

A significant concern lies with high-voltage power transformers (HVPTs), which form the backbone of bulk power transmission. Roughly 10–15% of HVPTs operating in the U.S. today are imported directly from China, including units deployed at critical substations and interconnects between regional grids.[23] Given the limited domestic manufacturing capacity for HVPTs and the long lead times associated with their replacement, any compromise of these assets—whether via embedded digital components or sabotage during manufacture—could have widespread consequences.

Another area for consideration is the widespread adoption of distributed energy resources (DERs), such as solar photovoltaics and associated inverters, which are frequently sourced from Chinese manufacturers. Inverter-based resources introduce bidirectional power flows and dynamic grid interactions. Many Chinese inverters include remote management capabilities, cloud-connected diagnostics, and over-the-air firmware updates—all potential vectors for exploitation or disruption if these systems are compromised.[24]

As the grid modernizes, energy management systems, smart meters, and advanced metering infrastructure (AMI) are also increasingly sourced from Chinese vendors. These systems collect

---

[23] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Large Power Transformers and the U.S. Electric Grid (Apr. 2014), https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf

[24] Megan J. Culler et al., BESSIE: Battery & Energy Storage Supply Chain Analysis, Mitigation Deployment, and Tools, INL/MIS-24-82394-Revision-0, Idaho Nat'l Lab. (Dec. 2024), https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65687.pdf

granular usage data, interface with control networks, and serve as gateways for utility-customer interactions. The presence of foreign-developed software in these tools, particularly if updated or serviced remotely, may enable long-term data harvesting or command injection.

Further, Chinese dominance in the battery energy storage market—estimated at over 70% of global supply—has led to large-scale deployment of PRC-made control systems in energy storage units nationwide.[25] These devices, now essential for peak shaving, black start operations, and renewable integration, represent both a cybersecurity and resilience risk if not properly isolated, monitored, and tested.

Continued reliance on untrusted foreign equipment creates opportunities for embedded threats, difficult-to-detect supply chain tampering, and coercive leverage during geopolitical crises. Reducing this risk requires a national strategy that includes repatriating key manufacturing capabilities, diversifying trusted suppliers, and ensuring full software and firmware transparency for all energy infrastructure components.

**Risks in Third-Country Infrastructure**

The cybersecurity risks posed by Chinese involvement in the infrastructure of third-party nations represent a significant and growing threat to U.S. national security and global energy stability. Through investment, technology transfer, and strategic partnerships, the People's Republic of China (PRC) has become a dominant force in the global buildout of energy and telecommunications infrastructure across Africa, Southeast Asia, Latin America, and parts of Eastern Europe. This international footprint allows China not only to extend its economic and diplomatic influence, but also to embed technologies that may carry security vulnerabilities or enable future remote access.

Much of this expansion occurs under the umbrella of the Belt and Road Initiative (BRI), which includes significant energy-sector investments such as power generation, substation automation, high-voltage transmission systems, and grid control platforms. Chinese state-owned enterprises (SOEs), such as State Grid Corporation of China and China Southern Power Grid, often lead these projects, deploying equipment and supervisory control and data acquisition (SCADA) systems that are developed domestically. The embedded software in these systems frequently lacks third-party vetting, relies on proprietary protocols, and is subject to PRC cybersecurity laws requiring cooperation with Chinese intelligence services.[26]

---

[25] Global Top 10 Power and ESS Battery Shipments Announced, Six Chinese Companies Hold Nearly 70% Market Share, Metal.com (Mar. 19, 2025), https://news.metal.com/newscontent/103195500/Global-Top-10-Power-and-ESS-Battery-Shipments-Announced-Six-Chinese-Companies-Hold-Nearly-70-Market-Share

[26] Michael R. Pompeo, Sec'y of State, Comm'n on Unalienable Rts., Safeguarding Our Freedom in the Digital Age (July 2020), https://it.usembassy.gov/secretary-pompeo-speech-at-the-national-constitution-center-july-16-2020/

This pattern creates two primary concerns. First, countries adopting PRC-supplied energy systems may unknowingly introduce persistent surveillance or remote-access risks. Second, these platforms can serve as launch points for lateral attacks or intelligence collection on U.S. allies and partners. For example, a compromised SCADA system in a foreign substation may offer visibility into regional grid flows, load patterns, or interconnection statuses that are relevant to U.S. diplomatic, military, or commercial activities in the area.

Recent cybersecurity advisories have highlighted that Chinese state-sponsored actors such as Volt Typhoon. These campaigns have been linked to anomalies in network traffic and operational disruptions, raising concerns about potential backdoor access facilitated through foreign infrastructure projects.[27] The United States and allied intelligence services have also expressed concern over Huawei's role in the deployment of smart grid communications infrastructure in strategic regions, particularly where those deployments coincide with military installations or sensitive resource corridors.

Beyond surveillance and cyber exploitation, Chinese investments in energy infrastructure also pose risks of operational coercion. The PRC has, in prior geopolitical disputes, restricted exports of rare earth materials or critical components. A similar leverage model could be applied to maintenance contracts, software updates, or spare parts necessary for grid reliability in third-country systems.

**Risk Mitigation When Alternatives Are Limited**

In certain segments of the energy sector, avoiding the use of Chinese-made components may be infeasible in the short term. Mitigation strategies must therefore account for existing dependencies while pursuing longer-term goals of supply chain diversification and domestic manufacturing capacity expansion.

1. A layered defense approach begins with rigorous supply chain risk assessments. Utilities and energy developers should identify all Chinese-origin components within their critical systems and evaluate their network exposure, remote access potential, and firmware update paths. Components with remote connectivity should be segmented on isolated networks, with strict firewall rules and no outbound internet access unless absolutely necessary.[28]
2. When foreign-manufactured components cannot be removed immediately, entities should implement cyber-informed engineering (CIE) practices. This proven approach, advocated by Idaho National Laboratory and the Department of Energy, focuses on designing grid systems

[27] U.S. Cybersecurity & Infrastructure Sec. Agency, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (Feb. 7, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[28] Nat'l Inst. of Standards & Tech., NIST Special Publication 800-82 Rev. 3, Guide Operational Technology (OT) Security (Sep 2023), https://doi.org/10.6028/NIST.SP.800-82r3

that limit the potential impact of cyber-initiated failures by incorporating fail-safes, manual overrides, and operational redundancies.[29]

3. Utilities should mandate firmware integrity checks and behavior baselining for field-deployed equipment. Any deviations from expected device behavior—such as unusual data transmissions, time drift, or reboots—should trigger alerts and forensic review. Modern network monitoring platforms that include asset fingerprinting, passive traffic inspection, and anomaly detection can help detect compromised devices operating within normal parameters.
4. Utilities and regulators should demand full transparency from suppliers regarding the origin and development of software and firmware. Where full software bill of materials (SBOM) disclosure is not available, utilities should treat such equipment as untrusted and isolate accordingly.
5. National programs should fund the development and deployment of Trusted Energy Infrastructure Zones (TEIZs)—pilot projects or demonstration areas where only hardware and software from vetted domestic or allied suppliers are allowed. These zones can serve as proving grounds for high-trust architectures and highlight the operational benefits of secure-by-design principles.
6. Several partner nations—such as India, Australia, and several EU member states—have begun excluding PRC vendors from critical infrastructure procurements. The United States has a strategic interest in supporting these decisions through technical assistance, capacity building, and the promotion of secure-by-design alternatives. Moreover, ensuring that regional partners adopt strong supply chain risk management practices—including source-code review, firmware validation, and contract enforcement mechanisms—can further reduce systemic exposure.
7. Where full replacement is not possible due to cost or availability constraints, the government should support compensating controls, such as hardened perimeter defenses, restricted control logic, physical separation, and tamper detection. These measures do not eliminate risk but can reduce the likelihood and impact of exploitation.

While perfect security is unattainable, meaningful reduction of systemic risk is achievable. Doing so requires a holistic strategy that combines technical safeguards, rigorous oversight, and policy coordination—especially where Chinese technologies remain embedded in the energy supply chain.

**Policy Recommendations**

To counter the growing risks posed by reliance on Chinese-manufactured equipment and state-sponsored cyber operations, the United States must adopt a comprehensive and sustained policy

[29] Emma Stewart et al., Applying Cyber-Informed Engineering to Grid Modernization, INL/EXT-21-63527, Idaho Nat'l Lab. (Aug. 2021), https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_147023.pdf

response. This response must span procurement, regulation, public-private coordination, and international engagement. Below are several recommended policy actions, rooted in both current threat intelligence and infrastructure realities:

1. **Reduce Exposure to High-Risk Components and Mandate Cyber-Informed Engineering.**
   Acknowledging that full-scale "rip and replace" is infeasible in the near term, the U.S. should focus on isolating, segmenting, and monitoring Chinese-manufactured components most susceptible to compromise. In parallel, Congress should mandate the application of Cyber-Informed Engineering (CIE), at a minimum for systems integrating foreign-sourced digital components. CIE ensures operational safety and mission continuity even if digital compromise occurs. While more resource-intensive, CIE offers a realistic path to resilience and should be funded accordingly.[30]
2. **Modernize Regulatory Frameworks for a Changing Grid.**
   We must continue to expand and modernize our regulatory frameworks. The NERC CIP standards provide a baseline for bulk power system reliability and cybersecurity, but they only apply to larger generation and transmission assets. As our grid evolves, new classes of risk are emerging in distributed energy aggregators, edge-connected devices, and vendor-controlled assets outside the traditional compliance footprint. Some voluntary standards are gaining ground, but currently, there is no top-level governance mechanism to bring many of these technologies under a unified security model. Addressing these gaps may require new regulatory or similar compliance frameworks for the creation of modern, fit-for-purpose standards that reflect the complexities and interdependencies of today's electric grid.
3. **Require Transparency in Firmware and Software Codebases.**
   Vendors supplying digital equipment to the bulk electric system or major distribution systems should be required to provide attestation of secure development practices, code origin audits, and third-party software composition analysis. Standards developed by NIST's Secure Software Development Framework (SSDF) and DOE's Cyber-Informed Engineering principles offer a strong foundation for these requirements.[31]
4. **Incentivize Domestic and Allied Manufacturing.**
   To reduce long-term dependence, Congress should expand tax incentives, loan guarantees, and public-private partnerships for domestic manufacturing of grid components. Coordinated industrial base strategies—such as those outlined in the CHIPS and Science Act—should be extended to transformer cores, HV relays, grid-scale inverters, and battery control systems.[32]

---

[30] Emma Stewart, Chief Power Grid Scientist, Idaho Nat'l Lab., Written Testimony Before the U.S. House Select Committee on the CCP, 118th Cong. (2024), https://democrats-selectcommitteeontheccp.house.gov/sites/evo-subsites/democrats-selectcommitteeontheccp.house.gov/files/evo-media-document/opening-statement-emma-stewart-final.pdf

[31] Nat'l Inst. of Standards & Tech., Secure Software Development Framework (SSDF) Version 1.1 (Feb. 2022), https://csrc.nist.gov/pubs/sp/800/218/final

[32] CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1392

5. **Enhance International Engagement and Standards Harmonization.**
   The U.S. should lead international efforts to develop aligned cybersecurity standards for energy equipment. Through organizations such as the International Electrotechnical Commission (IEC) and the International Energy Agency (IEA), the U.S. can push for common security requirements that reduce PRC influence in developing economies and Belt and Road recipient nations.
6. **Fund Targeted Testing and Reverse Engineering of Suspect Devices.**
   The Department of Energy, in coordination with National Laboratories, should assess the feasibility of developing and deploying trusted, open-source firmware for commonly used Chinese-manufactured energy equipment. In cases where hardware permits firmware replacement, this approach could mitigate embedded software risks while preserving utility investments in physical infrastructure. The National Labs could also lead firmware reverse engineering, behavioral baselining, and secure re-implementation, coupled with firmware provenance monitoring and code audits. Findings should inform regulatory action, public alerts, and real-time risk mitigation strategies.
7. **Prepare Consequence-Based Contingency Planning.**
   Recognizing that some legacy equipment will remain in place, DOE, FERC, and NERC should develop operational contingencies and tabletop exercises simulating hostile exploitation of embedded Chinese devices. These exercises must test not only system restoration but also interagency coordination and attribution procedures.

The PRC has demonstrated its willingness and capability to integrate coercive cyber tools into the energy domain. The response from the U.S. government must be equally strategic and preemptive—matching the technical sophistication of the threat with institutional resolve and regulatory foresight.

## Summary

The security of the United States' energy infrastructure is not merely a technical concern—it is a foundational pillar of national strategy, economic competitiveness, and global leadership. In an era defined by great power competition, the electric grid has emerged as a strategic asset whose security underwrites every other critical capability, including military readiness, artificial intelligence advancement, and quantum computing development. These emerging domains will require unprecedented energy availability, reliability, and resilience—none of which can be assured while adversarial access to grid infrastructure remains unchecked and unmitigated.

Chinese state-aligned cyber actors have evolved from opportunistic information theft and espionage to persistent pre-positioning within U.S. energy systems and other critical infrastructures. Their ability to exploit vulnerabilities in control systems, firmware, and supply chain dependencies enables both intelligence collection and disruptive potential in future conflicts. This testimony has documented the extent to which such risks are no longer

hypothetical. From Volt Typhoon's infiltration of power and water systems to the global dissemination of PRC-controlled technologies via the Belt and Road Initiative, China's strategic intent to compromise energy infrastructure has become unmistakable.

Concurrently, the United States is at a strategic inflection point. The renewed emphasis on energy dominance—a cornerstone of recent national policy—recognizes that energy independence alone is insufficient if the technologies underpinning the grid are compromised by foreign control. Securing the grid against Chinese influence is now a prerequisite for sustaining leadership in AI, quantum science, and advanced manufacturing, all of which depend on secure, high-capacity power delivery. A compromised grid is a constrained future.

At present, the U.S. lacks a unified, actionable strategy to detect, isolate, and mitigate these embedded risks. Regulatory frameworks like the NERC CIP standards have laid a foundation, but they require enhancement, modernization, and continued enforcement to match the evolving threat landscape. Policy solutions must embrace both the near-term need for Cyber-Informed Engineering and the long-term necessity of reshoring manufacturing, auditing firmware integrity, and harmonizing international standards.

And finally, how do we fund the kinds of improvements discussed in this testimony? The reality is, the mechanisms for financing grid security investments are complex and uneven. The electric grid is subject to a variety of regulators, oversight models, and cost recovery rules. It’s a difficult and important conversation—and one that needs to happen if we want real, sustainable progress.

To delay action is to cede advantage. The United States must marshal a coordinated national response—combining legislative clarity, regulatory reach, industrial mobilization, and international alignment—to secure its energy infrastructure against adversarial compromise. Only then can the U.S. claim true energy dominance: not just in supply, but in sovereign control over the technologies that sustain the nation's most critical functions.