TESTIMONY OF

Harry Krejsa
Director of Studies
Carnegie Mellon Institute for Strategy & Technology

BEFORE

The House Energy & Commerce Committee, Energy Subcommittee

ON

Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid

December 2, 2025
Washington, DC

Summary Points

- The AI boom is creating unprecedented demand for electricity, driving a massive and digitally-native expansion of the U.S. power grid. This transformation could either bring vital security and resilience advantages with it, or merely paper over our grid's vulnerability to attack, particularly from China, whose hackers have already infiltrated our aging infrastructure.
- Defending our energy ecosystem—and the AI race it is powering—will require a whole-of-nation approach that integrates new, modern energy stakeholders with traditional national security leaders. Only by leveraging both perspectives can the United States simultaneously capitalize on the abundance and security potential of modern energy technologies, mitigate their sources of technical risk, and retake industrial leadership from China's early advantage in the field.
- Speed and adaptability must define our response. The convergence of AI and advanced energy infrastructure is evolving faster than our governance structures can keep up. Success will require:
  - Rethinking existing industry convening and coordination structures;
  - Adopting more dynamic risk and reward assessments to identify critical "linchpin technologies" (like batteries, smart inverters, or virtual power plants);
  - Combining public-sector threat intelligence with private-sector purchasing power to drive secure-by-design practices and streamline secure deployment; and
  - Accelerating R&D priorities on "leap ahead" technologies that can break our dependence on Chinese-controlled supply chains, like next-generation batteries, enhanced geothermal, advanced nuclear, or fusion energy.

Thank you Chairman Latta, Ranking Member Castor, and Members of the Committee for the opportunity to talk to you today about why the AI-driven transformation of our energy infrastructure is both our greatest near-term vulnerability and our best opportunity to build a more defensible grid. I am the research director for the Carnegie Mellon Institute for Strategy & Technology, and a specialist in US-China technological competition. I came to Carnegie Mellon from a tour in government spanning both the Trump Pentagon and the Biden White House, where I helped devise new military doctrine for offensive cyber operations, and then led the development of the National Cyber Strategy. That experience left me convinced that the People's Republic of China views our grid as a strategic target—and that the technologies now reshaping our energy system have become a new front in great power competition.

The Opportunity: The AI Infrastructure Buildout is a Golden Opportunity to Simultaneously Secure Our Grid and Power Our Future

Artificial intelligence's explosive growth is driving a historic transformation of America's energy infrastructure. The booming expansion of data centers across the country is creating unprecedented electricity demand, and with it, historic levels of investment in our power grid that no other critical infrastructure sector enjoys.

Yet this AI-driven buildout is also arriving at a moment of profound vulnerability. Our aging grid is a hodgepodge of digital tools sitting atop an analog foundation that was never designed for modern levels of connectivity. The U.S. government has warned consistently that the PRC is seeking to exploit this tension. Chinese President Xi Jinping reportedly has directed the People's Liberation Army (PLA)—China's military—to be prepared to do just that in a conflict over Taiwan by the year 2027.[1] In anticipation of such a conflict, Beijing has been investing in cyber capabilities and operations intended to disrupt our critical infrastructure. Our inconsistent mix of older, insecure infrastructure and highly interconnected computer systems is creating "seams" in technology that are too easy for cyber actors to exploit.

Exploiting these "seams" during a crisis would have both military and civilian costs. Leaders from the Cybersecurity and Infrastructure Security Agency (CISA) have testified to Congress[2] that PRC cyber actors are seeking to preposition disruptive cyber effects on U.S. infrastructure to stymie Washington's ability to project power abroad while sowing societal chaos at home.[3] FBI leaders have similarly warned that these malicious cyber campaigns are "broad and unrelenting," and that Beijing's "plan is to land low blows against civilian infrastructure to try and induce panic and break America's will to resist.[4]" Recent research into cyberattacks against hospitals by criminal ransomware gangs suggests that even simple disruptions to computer services can meaningfully raise patient mortality rates; if paired with disruptions to water or power, it is easy to imagine how human consequences could worsen quickly within and beyond the healthcare system.[5]

Microsoft in 2023 publicly exposed one PRC state-backed hacking group responsible for a variety of critical infrastructure intrusions, issuing them the taxonomic moniker "Volt Typhoon[6]." Volt Typhoon was notable for its stealth, using a variety of means to secure a user's valid credentials and then wielding those credentials so that their nefarious activities blended into legitimate network traffic (cyber tradecraft known as "living-off-the-land techniques"). Volt Typhoon apparently has been active on U.S. systems since 2021 and motivated some of the federal government's most urgent recent warnings about the vulnerability of Americans' infrastructure.[7] With only 10-20% of our electricity system under federal cybersecurity oversight, a rapidly-diversifying industry ecosystem, and an outdated governance apparatus too fragmented to address systemic vulnerabilities, the status quo is dangerously untenable for both the AI race and our critical services.[8]

Yet this crisis presents us with a golden opportunity to pour a stronger foundation for both our public safety and our energy ambitions alike. The energy technologies overwhelmingly powering our recent grid expansion are far more digitally-native than what has come before, from on-site co-generation and battery storage to smart inverters and virtual power plants. These modern systems were designed from the ground up with software at their core, enabling modern cybersecurity features and the ability to update and evolve in response to emerging threats. These technologies are also shepherding a smarter, more distributed grid architecture—one that is not only more defensible, but also resilient and self-healing, capable of quarantining disruptions and preventing cascading blackouts.

Many of these modern technologies also promise a new frontier in energy security. Nuclear power, geothermal wells, inverter-based resources, and battery storage—the preferred energy sources for most tech giants, and the source of most new electricity being added to the grid—either require no or infrequent refueling, and in some cases even approach near-zero-marginal-cost electricity generation.[9] Being liberated from the ups and downs of commodity fuel prices would be a significant benefit for American energy consumers, who are facing significant increases in their utility bills. But this transformation would also be a valuable defense against a US-PRC contingency in the Indo-Pacific. Our allies and partners in the region, upon whose grids our own forward-deployed forces rely, are heavily dependent on maritime fuel shipments for their electricity. Modern and digitally-native energy technologies promise to be not only more defensible against the kinds of cyberattacks we know Beijing is planning against our allies, but also more resilient against blockades and other naval risks that fragile oil and gas tankers will likely face in any such conflict.

The Urgency: AI Competition is Taking Center Stage in US-China Competition – and Painting A Target On Our Grid

But as the AI boom brings more opportunities to harden our grid against attack, it may also increase the interest of potential attackers. Compute power is directly and increasingly tied to

electricity availability, making our grid the strategic chokepoint in the race for artificial intelligence advantage. As Beijing recognizes the strategic implications—especially after tools like DeepSeek, Qwen, and Kimi demonstrated China's formidable AI capabilities—it will likely paint an even bigger target on our energy infrastructure and increase their and others' risk tolerance for more aggressive cyber operations. The shift from training-intensive to inference-intensive AI compounds this challenge, as compute requirements diffuse from remote mega-centers to more distributed, latency-sensitive facilities closer to everyday Americans—and potentially growing our compute infrastructure's attack surface in the process.

While the United States has a narrow lead in the AI race for now, China has secured an advantage in the swift, cheap deployment of electricity that will power the race into the future. Beijing has used its early capture of smartphone and electronics manufacturing to dominate what some are calling the "electrotech stack"—the foundational components that underpin modern energy systems, AI infrastructure, robotics, and many other technologies that will likely be key to future innovation and growth.[10] Beijing controls the majority of global battery production, precision magnets, power electronics, and other critical components that were refined and miniaturized during the smartphone revolution and now define the digitally-native energy future. These cascading advantages mean that even as the United States races to deploy modern energy technologies to power our AI ambitions, we remain dangerously dependent on the very actor from whom we need to defend our grid. While federal investments retained in the One Big Beautiful Bill Act continue to support the standup of domestic battery manufacturing, advanced nuclear, and enhanced geothermal development, we are still playing catch-up in a game where China already has secured a considerable lead.

The convergence of energy and compute infrastructure around this shared electrotech heritage means that securing our AI future will require not just building more data centers or power plants, but fundamentally reconceptualizing, securing, and—where risk prioritization requires it—reshoring the component technologies that make both possible. Our policy and governance frameworks are dangerously unprepared for this convergence of opportunities and challenges accompanying the AI-driven grid transformation. Traditional infrastructure protection bodies have been slow to incorporate modern energy stakeholders, new market entrants are too often naive about security risks and supply chain dependencies, and no unified approach exists for the convergence of digital and legacy technologies that are reshaping our grid.

In my testimony today, I want to make the case that success requires urgent action and national leadership across three lines of effort:

- Unifying strategic priorities for the security, availability, and swift deployability of modern energy technologies;
- Organizing disparate modern energy and national security stakeholders across the public and private sectors; and

- Maintaining vigilance over fast-moving developments in both AI architectures and energy systems that could rapidly shift our security posture.

Taking these steps will ensure the public and private sectors are prepared to collaboratively secure the energy foundation for America's future while denying our adversaries the leverage to disrupt it.

The United States Needs unified, Strategic Priorities for the Security, Availability, and Swift Deployment of Modern Energy Technologies

Beijing clearly views its early lead in modern energy manufacturing, and its ability to rapidly deliver resilient and abundant electricity, as a strategic asset worth protecting. Chinese President Xi Jinping has repeatedly emphasized the need to coordinate "new energy" development alongside broader national security considerations, fusing its national security and economic impacts.[11] As global investment in these digitally-native technologies approaches $2 trillion annually, China has positioned itself at the center of one of history's largest capital opportunities—insulating itself from economic isolation while maintaining leverage over critical supply chains.[12] The United States must signal an equally serious political, financial, and security commitment to leadership in these technologies.

While Washington shouldn't reactively mirror Beijing's every move, it must recognize when our competitors are right: Modern, digitally-native energy technologies are not just trendy nice-to-haves, but strategic imperatives for maintaining competitiveness in both the AI race and the broader contest for technological leadership.

<u>Recommendation</u>

The Committee should consider how to ensure the U.S. government adopts a whole-of-nation strategy to guarantee the security, availability, and vendor trustworthiness of the modern energy technologies that will be key to powering the AI race and subsequent engines of innovation.

- This strategy should focus in the near term on the cybersecurity of key modern energy technologies (especially those with high dependence on PRC supply chains) and scalable solutions to promote the faster deployment of secure and resilient electricity.
- For the medium term, it should adapt lessons learned from U.S. and allied semiconductor supply chain diversification efforts, including maintaining both leading-edge innovative engines to maintain advantage as well as trailing-edge production capacities to hedge against supply disruption.
- This strategy should prioritize maintaining U.S. and allied leadership in international energy technology financing. This should ensure that cyber-secure and trusted technology is accessible to emerging markets, that those markets' demand can contribute to scaling U.S. and allied manufacturing capacity, and in so doing, balance PRC influence over the

future of those markets' energy security so we avoid another Huawei-and-5G-style setback.[13]

We Need Federal Leadership to Organize Disparate Modern Energy and National Security Stakeholders Across the Public and Private Sectors

The development, security, and deployment of modern energy technologies is increasingly intertwined with US-China competition, but the communities driving each remain dangerously siloed. Traditional energy and security stakeholders possess decades of experience mitigating national security threats, but are poorly integrated with the entrepreneurs and innovators deploying digitally-native technologies that now make up the majority of new electricity generation. Meanwhile, modern energy developers—often smaller, more numerous, and less security-sophisticated than their traditional counterparts—are racing to deploy sophisticated software-defined systems without adequate access to threat intelligence or security frameworks. This disconnect extends throughout our governance structures: Public-private critical infrastructure protection bodies have not updated their frameworks to address the fundamentally distinct way modern energy technologies interact with digital connectivity, while energy policy processes deploy grid-transforming technologies with minimal integration of national security expertise.

The convergence of AI compute and rapidly-digitizing energy infrastructure demands a more integrated community of practice around the risk of Chinese tech dependencies that can transform sources of potential technical vulnerability into strategic advantage, but will require leadership from the federal government and industry executives to succeed.

Recommendation
The Committee should consider how to ensure the U.S. government intentionally integrates relevant national security and modern energy policymaking processes and frameworks.

- Given the rapidly growing importance of modern, digitally-native technologies to our grid, the National Energy Dominance Council—and other relevant energy-focused policymaking bodies and processes—should include CISA and the National Security Agency in its membership.
- The next National Infrastructure Risk Management Plan, a White House-directed policy update coordinated by CISA, should explicitly incorporate the novel considerations introduced by modern energy technologies.

Recommendation
The Committee should consider how to ensure industry coordination and intelligence distribution bodies, like Information Sharing and Analysis Organizations and Centers (ISAOs/ISACs),

update their membership and processes to incorporate and engage with the modern energy ecosystem and its structural novelties.

- ISAOs/ISACs should review a) their membership to ensure they reflect the modern, digitally-native energy influence in their marketplaces, and b) restructure their coordination mechanisms to better integrate with smaller, more numerous, and less risk-sophisticated modern energy stakeholders.
- ISAOs/ISACs and sector-specific coordinating councils should adapt security and resilience resources for modern energy stakeholders' unique considerations, including those on secure-by-design principles, technical standards implementation, and open-source software security.

Recommendation

The Committee should consider how electricity sector stakeholders, from utilities to the tech industry, can drive coordinated cybersecurity practices that are tailored to and scalable among the broader modern energy marketplace.

- The country's energy utilities and infrastructure operators should coordinate on shared guidance for "what right looks like" for the unique cybersecurity considerations of integrating digitally-native energy technologies into their grids. This will make it easier for more modern energy vendors to scale their contributions to security and resilience across different regional regulatory jurisdictions and integrate into different regional grids more quickly, all while helping mitigate broad regulatory gaps in electricity infrastructure cybersecurity.
- Cloud computing hyperscalers, whose next-generation AI training and inference data centers are helping to propel historic increases in electricity demand, should use their purchasing power to inform and drive new modern energy cybersecurity practices. As some of the few actors in the U.S. economy possessing deep expertise in both energy economics and PRC exploitation of flawed software, today's AI-driven hyperscalers should use their influence over the next generation of energy deployment to inform and drive the development of modern energy-specific security practices.

Industry and Government Must Remain Nimble to – and Vigilant of – Fast-Moving Developments in Both AI architectures and Energy Systems That Could Rapidly Shift Our Security Posture

The convergence of AI and modern energy infrastructure is evolving at unprecedented speed, demanding frameworks that can adapt as quickly as the technologies they govern. Just years ago, batteries were peripheral to grid planning—today they keep entire states' grids operational during peak demand.[14] The shift from training-intensive to inference-intensive AI is similarly upending assumptions about data center geography, latency requirements, and co-located generation needs. Our prioritization frameworks must be equally dynamic, capable of rapidly

reassessing which technologies pose the greatest systemic influence—and bring the most digital risk—as the landscape shifts. Virtual power plants, for example, are entirely software-defined with massive systemic impact, yet their digital nature may make them easier to secure through established software validation practices—if we act quickly. Batteries present a more complex challenge: digitally sophisticated enough to pose risk, systemically critical to grid stability, yet often dependent on Chinese supply chains that challenge traditional security controls. Meanwhile, breakthroughs in solid-state batteries, enhanced geothermal, or fusion reactors could suddenly offer leap-ahead opportunities to break supply chain dependencies—but only if policymakers are watching for them.

As specific technologies and threats evolve, certain principles must endure: prioritizing the security of our most systemically critical infrastructure, maintaining vendor trust and supply chain awareness, and ensuring that every new deployment enhances rather than undermines our grid's defensibility against adversary attack. But in this current environment, our greatest risk may be fighting yesterday's war with outdated assumptions about where threats and opportunities lie. To operationalize this balance between enduring priorities and adaptive flexibility, we need assessment frameworks that are rigorous enough to guide billion-dollar infrastructure investments yet nimble enough to evolve with the rapidly shifting AI-energy landscape. These frameworks must evaluate both relative risk—assessing digital exposure and systemic influence across technologies—and difficulty of remediation—identifying which vulnerabilities can be addressed through scalable interventions, versus those requiring bespoke solutions.

This will require a more nimble approach to risk assessment and technology development—one that can identify which emerging technologies pose the greatest security exposure while simultaneously spotting opportunities to break free from geopolitically risky dependencies. We need frameworks agile enough to continuously reassess the threat landscape as new technologies achieve critical mass, yet rigorous enough to guide major infrastructure investments. Equally important, we must actively cultivate breakthrough alternatives—like in solid-state batteries, enhanced geothermal, or advanced nuclear and fusion—that could provide leap-ahead substitutes for the PRC-dominated components that define our energy supply chains. The U.S. government should work with industry to establish assessment mechanisms to track this evolving landscape, and R&D priorities to shape it in America's favor.

Recommendation

The Committee should consider how to ensure the Office of the National Cyber Director, Department of Energy, CISA, and the National Security Agency develop a joint risk and

remediation framework for modern energy technologies that can inform legislative priorities for onshoring initiatives and sourcing from Foreign Entities of Concern.

- The assessment should recognize "linchpin technologies" key to our AI-driven grid buildout according to digital exposure, systemic impact, and relevant threat intelligence. It should identify areas of scalable interventions for swifter and more secure deployment—such as with broader adoption of certain secure software development practices—and areas where bespoke interventions may be required.
- The assessment should consider near-term cybersecurity considerations as well as longer-term supply chain dependencies that may impede greater certainty in relevant technologies' security and resilience. These can better inform investment and manufacturing tax credits and other Congressional actions to shape our evolving energy technology ecosystem.

Recommendation

The Committee should consider how to ensure the Office of Science & Technology Policy, the Department of Energy, and the Department of Commerce establish an R&D strategy for modern energy technologies that not only are game-changing generation and storage tools, but also provide "leap-ahead" substitution opportunities for U.S. and allied manufacturers currently dependent on PRC supply chains and electrotech advantages.

- This R&D strategy should identify and accelerate emerging technologies that could help break U.S. and allied dependence on vulnerable or insecure supply chains.
- This strategy should adjudicate for which technologies the United States is willing to tolerate relative PRC dominance—perhaps including, for example, relatively "dumb" and commodity energy components—and those that are more systemically impactful and over which the United States should seek to retain influence and Congress can legislate such inducements, such as in battery storage or other more digitally-native platforms.

Conclusion

Chairman Latta, Ranking Member Castor, and Members of the Committee: the question before us is not simply how to defend an aging grid against cyber and physical threats—it is whether the United States will seize a once-in-a-generation opportunity to build something stronger in its place. The AI-driven transformation of our energy infrastructure is happening now, with or without deliberate security leadership. Left unguided, this buildout risks entrenching our dependence on adversary-controlled supply chains and expanding our attack surface at the very moment Beijing is positioning to exploit it. But approached strategically—with unified priorities, organized stakeholders, and adaptive vigilance—this same transformation can yield an energy foundation that is not only more abundant and affordable, but fundamentally more defensible than what came before. The technologies powering the AI race were designed for the digital age;

our governance and security frameworks must be as well. Thank you for the opportunity to discuss these issues before the Committee today.[15]

---

[1] "Statement of Admiral John C. Aquilino, U.S. Indo-Pacific Command, on U.S. Indo-Pacific Command Posture, to the U.S. House Armed Services Committee," Congress.gov, 20 March 2024, https://www.congress.gov/118/meeting/house/116960/witnesses/HHRG-118-AS00-Wstate-AquilinoJ-20240320.pdf.
[2] Formally, "Select Committee on Strategic Competition Between the United States and the Chinese Communist Party"
[3] "Testimony of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, on the CCP Cyber Threat to the American Homeland and National Security, to the Select Committee on Strategic Competition Between the United States and the Chinese Communist Party," Congress.gov, 31 January 2024, https://docs.house.gov/meetings/ZS/ZS00/20240131/116776/HHRG-118-ZS00-Wstate-EasterlyJ-20240131.pdf.
[4] "Wray: Chinese government poses 'broad and unrelenting' threat to U.S. critical infrastructure." FBI, 18 April 2024, https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says.
[5] Zac Amos, "The Link Between Health Care Cyberattacks and Patient Mortality," The Journal of mHealth, 8 January 2024,, https://thejournalofmhealth.com/the-link-between-health-care-cyberattacks-and-patient-mortality/.
[6] "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft Security Insider, 25 May 2023, https://www.microsoft.com/en-us/security/security-insider/emerging-threats/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques.
[7] Julian E. Barnes, "China Could Threaten Critical Infrastructure in a Conflict, N.S.A. Chief Says," The New York Times, 17 April 2024, https://www.nytimes.com/2024/04/17/us/politics/china-cyber-us-infrastructure.html.
[8] "Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems," Government Accountability Office, March 2021, GAO-21-81, https://www.gao.gov/assets/gao-21-81.pdf; "Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid," Government Accountability Office, August 2019, GAO-19-332, https://www.gao.gov/products/gao-19-332.
[9] Dan McCarthy, "Chart: 96 percent of new US power capacity was carbon-free in 2024," Canary Media, January 2025, https://www.canarymedia.com/articles/clean-energy/chart-96-percent-of-new-us-power-capacity-was-carbon-free-in-2024.
[10] Daan Walter, Sam Butler-Sloss, and Kingsmill Bond, "Rewiring the Energy Debate," The Electrotech Revolution, May 2025, https://electrotechrevolution.substack.com/p/rewiring-the-energy-debate.
[11] "Xi Jinping Emphasizes Vigorously Promoting High-Quality Development of New Energy in China to Make Greater Contributions to Building a Clean and Beautiful World during the 12th Collective Study Session of the CCP Central Politburo," CSIS Interpret: China policy document translation, published by Xinhua News Agency, 29 February 2024, https://interpret.csis.org/translations/xi-jinping-emphasizes-vigorously-promoting-high-quality-development-of-new-energy-in-china-to-make-greater-contributions-to-building-a-clean-and-beautiful-world-during-the-12th-collective-study-sessio/.
[12] Executive Summary of the World Energy Outlook 2024, International Energy Agency, October 2024, https://www.iea.org/reports/world-energy-outlook-2024/executive-summary.
[13] Brian Deese, "The Case for a Clean Energy Marshall Plan: How the Fight Against Climate Change Can Renew American Leadership," Foreign Affairs, 20 August 2024, https://www.foreignaffairs.com/united-states/case-clean-energy-marshallplan-deese.
[14] Robert Walton, "Batteries are making the grid more reliable: NERC," Utility Dive, June 2025, https://www.utilitydive.com/news/batteries-grid-state-of-reliability-nerc/750649/; Garrett Golding, "Solar, battery capacity saved the Texas grid last summer; an uncertain future awaits," Federal Reserve Bank of Dallas, January 2025, https://www.dallasfed.org/research/economics/2025/0114.
[15] This testimony was adapted from recent research for the Carnegie Mellon Institute for Strategy & Technology.