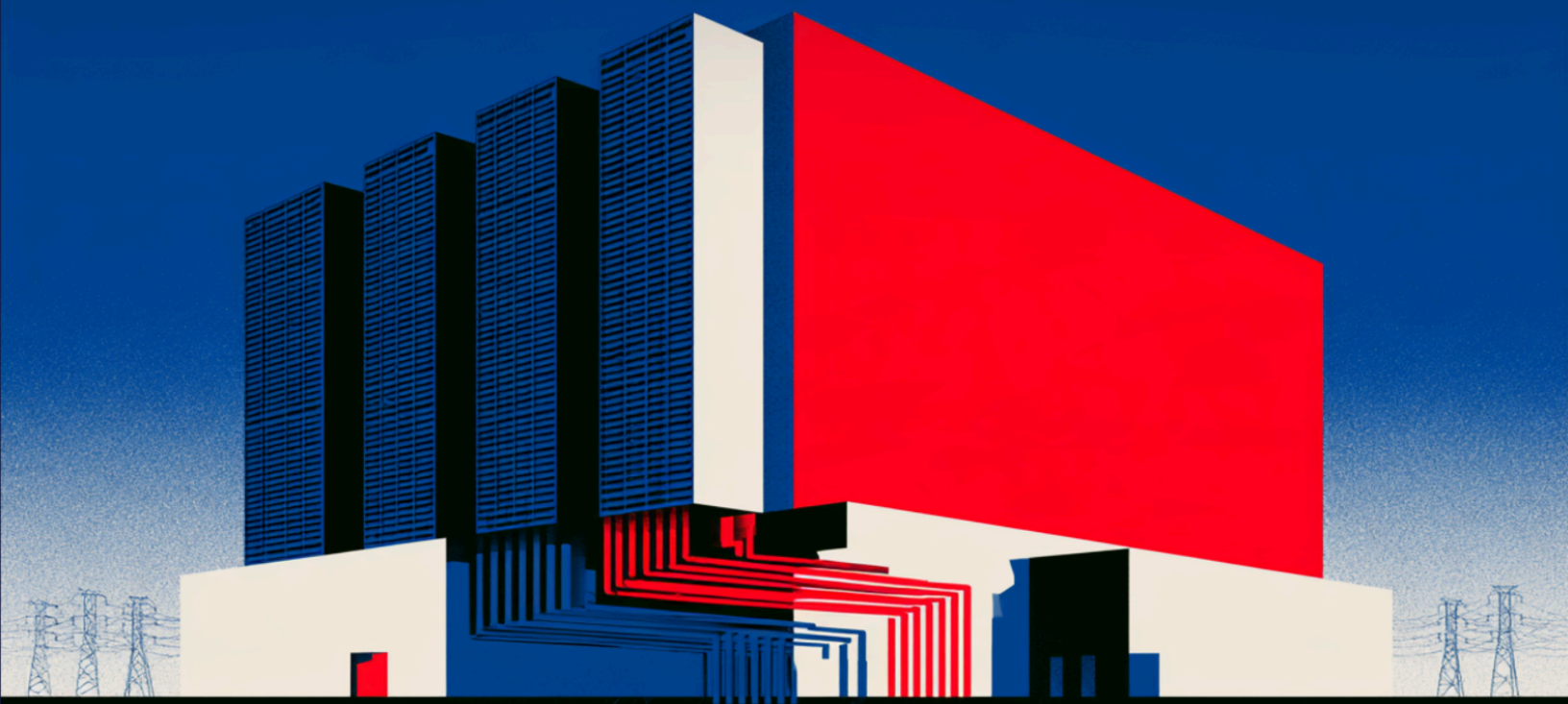
AMERICANS *for* RESPONSIBLE INNOVATION

THE INVISIBLE BACKBONE:

GIGAWATT JUGGERNAUTS:

How AI Infrastructure Expands the Energy Attack Surface



BY JESS MAKSIMOV

OCTOBER 2026

Executive Summary

As data center demand climbs to unprecedented levels, artificial intelligence (AI) developers depend on the reliability and security of U.S. energy generation, transmission, and distribution systems. This paper examines the AI sector's reliance on energy infrastructure and the vulnerabilities this interdependence brings. It is part of Americans for Responsible Innovation's Invisible Backbone Series, examining nation-state threats to the critical infrastructure that underpins AI. This paper follows the series opener,[1] which defines the AI infrastructure sector and identifies it as a valuable nation-state target.

We analyze the vulnerabilities of five energy nodes that can present widespread risks if interdicted: natural gas networks, large power transformers (LPTs), control systems, grid-enhancing technologies (GETs), and select data centers' microgrids. Natural gas supplies over 40 percent of U.S. data center electricity.[2] LPTs convert the high-voltage electricity zipping through interstate energy highways into lower voltage levels that data center campuses and clusters can use.[3] Control systems serve as utilities' digital nervous systems, sensing conditions and signaling grid disturbances to operators. GETs, though not yet widespread, determine how much supply can physically reach demand. And data centers' microgrids increasingly generate, store, and distribute power internally.

Each of these nodes carries documented vulnerabilities that a threat actor can exploit to degrade U.S. AI capabilities. Natural gas pipelines rely on operational technology that can be remotely accessed. LPTs are custom-built and subject to lengthy replacement timelines of two to four years. Control systems depend on communications networks that adversaries have already penetrated. GETs display data-integrity vulnerabilities. And facility-level microgrids add new cyber entry points within the very backup systems that are meant to provide resource redundancy. Compounding these vulnerabilities, data center clusters concentrate voltage-sensitive, inflexible large loads behind energy chokepoints, where a single interdiction can cascade across many facilities.

To safeguard the infrastructure at the energy-AI nexus, the U.S. government must designate AI as a critical infrastructure sector to open a security coordination mechanism between the AI industry, federal agencies, and energy stakeholders; grant Sector Risk Management Agencies (SRMAs) the authority to set baseline security standards for vulnerable infrastructure; run wargames to sharpen cross-sector threat detection and response; and create reliability standards for data center loads, compelling utilities and data center operators to deploy secure-by-design control systems and GETs in areas serving data center clusters.

Introduction

Over the last decade, Berserk Bear—a Russia-linked threat actor—has permeated energy infrastructure backbones to conduct reconnaissance on U.S. industrial systems.[4] In December 2015, the attackers sent seemingly innocent New Year's Eve invitations to energy sector workers. Once these jovially masqueraded emails were opened, the attached document leaked the victims' network credentials into a separate server, where Berserk Bear recovered the passwords. The group then used these credentials as camouflage to enter the organization's internal networks. Simultaneously, Berserk Bear compromised the websites that energy workers frequently visited by using trojanized software to penetrate walled networks and installing backdoors to give the attackers access to their victims' computers. Once inside the walled cities of peripheral organizations, Berserk Bear conducted reconnaissance and opened the door to its intended victims' systems.

Once again, the group gathered unsuspecting users' credentials. Now inside the targets' networks, Berserk Bear surveilled operations and secured access to the corporate network servers housing data from energy facility control systems. In the most successful instances, the attackers gained sufficient access to screenshot their targets' control panels.[5] Eric Chien, a Symantec cybersecurity analyst, noted, "You'd take these sorts of screenshots to understand what you had to do next, like literally which switch to flip."[6] This operation went on for years, permeating intertwined U.S. systems to target critical infrastructure, exploiting vulnerabilities in one sector (information technology) to target another (energy).

But Berserk Bear was not the only actor burrowing into U.S. networks. In 2024, a government advisory revealed that the People's Republic of China (PRC)-linked Volt Typhoon group had pre-positioned its access within U.S. critical infrastructure networks, creating the conditions for a sudden, widespread attack.[7] Meanwhile, PRC-linked Salt Typhoon was conducting an espionage campaign and compromising U.S. telecommunications companies' networks to steal customer call records, politicians' private communications, and U.S. law enforcement information.[8]

Against this vulnerability-riddled backdrop,[9] new artificial intelligence (AI) infrastructure is coming onto the grid, introducing new failure points: First, as the series opener argues, the data centers housing AI workloads are becoming valuable targets for nation-states, whose attacks are the focus of this series.[10] Second, data centers bring energy vulnerabilities because of their large loads, inflexible profiles, voltage-sensitive controls,[11] and facility-level microgrids.[12] As data centers connect to a grid where state-linked intruders have already mapped out the cybersecurity landscape,[13] the energy-AI infrastructure attack surface grows.[14]

AI's Achilles' Heel: Energy Chokepoints and Vulnerabilities

ARI's Invisible Backbone Series opener defines AI infrastructure across five layers: model development and software; compute; hardware design and manufacturing; operational and delivery systems; and purpose-built assets, such as data centers' on-site generation.[15] Through this lens, AI is itself an infrastructure sector that depends on the U.S. energy system to power its services. As AI operations proliferate and data center demand climbs into the gigawatts (one gigawatt alone powers upwards of 800,000 households),[16] these facilities need reliable and secure energy generation, transmission, and distribution to function. This section follows the energy system from the wellhead to the server rack to examine the nodes that electrons pass through along the way. The paper identifies four existing and one emerging chokepoint, where a single interruption could produce effects that are wide, slow to reverse, and concentrated on AI facilities.

Demand at the Server Rack

Two data center load features make these facilities particularly susceptible to energy chokepoints: their scale and geographical concentration. A 2025 Idaho National Laboratory (INL) study sets the threshold for a "large load" at 50 megawatts of real power.[17] Above that level, in most regions, hourly demand markets alone cannot compensate quickly enough if the load suddenly disconnects ("drops") from the grid. But hyperscale data center campuses now exceed this threshold, requiring hundreds of megawatts.[18] Data centers are also emerging in clusters around the country, in regions such as Texas and the Mid-Atlantic—home to Data Center Alley in Northern Virginia.[19] Nearly half of all data center capacity in the United States is concentrated in just five regional clusters, and 50 percent of all new data center construction is sited in pre-existing clusters—resulting in concentrated AI infrastructure chokepoints along the energy network.[20] Tracing that network, the first chokepoint is the fuel that powers most data centers.

Natural Gas

Natural gas is the largest single source of electricity for U.S. data centers, supplying over 40 percent of their power.[21] The International Energy Agency (IEA) projects that gas will constitute the greatest share of new U.S. supply to these facilities through 2030.[22] Data center dependence on this energy source is seen both in front of the meter (power drawn from the grid) and behind the meter (generation serving the data center directly), with the IEA projecting that approximately 15–27 gigawatts of on-site natural gas may power U.S. data centers by 2030.[23]

In a 2025 "Reliability Risk Priorities" report, the North American Electric Reliability Corporation (NERC)—the grid reliability watchdog—finds that pipeline development is not keeping pace with the scale of grid transformation driven by new large loads and energy sources connecting to the grid.[24] NERC's report also warns that the extended lead times for new generation procurement, assembly, and installation are further compounding these constraints.[25]

Documented physical and cyber attacks on U.S. natural gas and oil networks already reveal the vulnerabilities that attackers can exploit to target the data center clusters. In 2021, threat actors executed a ransomware attack on the corporate IT billing system of the Colonial Pipeline, which delivers roughly 45 percent of the fuel consumed on the U.S. East Coast.[26] Colonial had to shut down

its 5,500-mile pipeline for six days, causing fuel shortages up and down the coast.[27] In addition, according to the Cybersecurity and Infrastructure Security Agency (CISA), U.S. pipeline infrastructure increasingly depends on automation to drive its operations efficiently and reliably.[28] CISA warns that pipeline IT and operational technology (OT)—systems that manage physical infrastructure—add new vulnerabilities that attackers could exploit to cause "explosions, equipment destruction, unanticipated shutdowns or sabotage, theft of intellectual property, and downstream impacts to National Critical Functions."[29] In 2020, CISA issued an alert detailing a ransomware attack on the control and communication assets of a natural gas compression facility (a plant that increases natural gas pressure to enable its flow through pipelines), which led the operator to implement a "deliberate" two-day shutdown of its operations, resulting in productivity and revenue losses.[30]

Actors have also exploited physical entry points along the U.S. pipeline network. In 2016, climate activists temporarily disrupted five pipelines transporting oil from Canada to the United States by closing their manual safety valves.[31] In 2017, activists damaged the Dakota Access Pipeline by torching holes through the line and setting fire to its equipment.[32] These incidents required minimal resources and little technical sophistication, but nation-state actors could amplify this threat, bringing dedicated resources and the expertise needed to map and exploit such vulnerabilities systematically.

Large Power Transformers

Almost every watt of power a data center draws from the grid must pass through a large power transformer (LPT), which can serve thousands of customers or entire data center campuses.[33] The U.S. Department of Energy reports that over 90 percent of all consumed power passes through LPTs, noting that their loss "could disrupt electricity services over a large area of the country," making LPTs a vital and vulnerable node powering AI infrastructure.[34]

LPTs are custom-built and have long replacement lead times, making them high-value physical targets for an attacker seeking to cause prolonged disruptions in regions where LPTs serve many data centers. In 2024, CISA's National Infrastructure Advisory Council (NIAC) found that LPT supply chain constraints are creating wait times of two to four years for transformer replacements.[35] Moreover, as the grid's composition changes, rising transformer demand is spiking prices, making replacements more expensive.[36]

Attacks on LPTs are not a novelty.[37] In 2013, a rifle attack disabled 17 transformers in a substation serving Silicon Valley.[38] Surrounding power plants kicked in as operators rerouted power to avoid blackouts. The substation then remained offline for nearly a month.[39] Following the attack, NERC implemented a mandatory Physical Security Reliability Standard "to identify and protect" transmission substations from physical attacks.[40] But in the last decade, dozens more facilities have been targeted.[41] In 2022, another shooting at two substations in North Carolina left tens of thousands of residential and commercial customers without electricity for almost four days and impacted pharmacies, traffic lights, and businesses.[42]

The Electricity Information Sharing and Analysis Center (the energy sector's threat-intelligence hub) found that physical security incidents, such as ballistic damage, intrusions, and cut wires, occur every year, impacting grid operations. The Center also determined that, in 2024, 37 percent of grid-impacting incidents were likely sabotage.[43] These disruptions demonstrate how attacks on energy chokepoints could bring widespread impacts that cascade through communities.

Control Systems

Control systems are vital for monitoring AI data centers' energy demand. AI data centers' unpredictable load behavior challenges the grid's stability,[44] as the loads "can exhibit sharp, short-term ramping behavior that varies by the hour or even minute."[45] Such fluctuations can contribute to cascading failures across the grid, impacting nearby data centers in clustered regions.[46]

Many data centers also have limited load flexibility, so they cannot automatically adjust their power consumption in response to grid conditions without impacting internal operations.[47] INL researchers highlight that data centers require "high, continuous power" and "24/7 availability with minimal tolerance for outages or voltage fluctuations."[48] Even brief outages can cost up to $9,000 per minute of data center downtime.[49] Therefore, data center facilities use voltage-sensitive responses, allowing them to quickly detect and respond to grid disturbances.[50] In 2024, for example, a failed surge protector on the Eastern Interconnection in Northern Virginia sent 1,500 megawatts of data center loads tumbling off the grid, switching to on-site generation within milliseconds and leaving operators scrambling to respond.[51]

As these clustered, voltage-sensitive juggernauts come online, operators must navigate a new terrain while maintaining stable power for all energy consumers. Control systems help gather real-time information and allow operators to supervise the grid as data center loads add new strain.[52] As large-load fluctuations accompany new data centers onto the grid, operators will likely require more voltage-control equipment throughout the transmission system, increasing their reliance on this technology during sub-minute demand fluctuations.[53]

According to NERC, the U.S. transmission system is also growing increasingly reliant on telecommunications networks for grid monitoring, remote control, emergency response, and system restoration.[54] Because control systems depend on accurate, real-time data to give operators field visibility and enable remote response to disturbances, their reliance on vulnerable networks gives threat actors a path into the grid—the same path Berserk Bear charted when it mapped energy controls from less-guarded peripheral organizations.[55]

Data Centers as Microgrids

Faced with an aging grid, lengthy infrastructure upgrade timelines, and limited transmission capacity,[56] data center developers are building their own microgrids with behind-the-meter generation, on-site storage, and facility-level control systems.[57] Data center operators are increasingly moving toward behind-the-meter generation, with 29 percent of surveyed data center executives already deploying on-site generation, another 39 percent planning to add on-site power within the next two years,[58] and 70 percent noting that they expect these power buildouts to "significantly" reduce their grid reliance.[59] Because these on-site systems run on the same sensors, software, and third-party platforms as grid control systems, they inherit the same vulnerabilities; however, as an increasing share of AI capacity moves behind the meter, the facilities' system security falls outside utility oversight.

Moreover, attackers could develop mechanisms to disrupt data centers' power stability from within the facilities themselves. Researchers have demonstrated that "Bit2Watt attacks" would allow threat actors to manipulate semiconductor workloads within a data center to induce power quality distortions that could disrupt internal operations. These attacks can stress data center power-delivery equipment,

trigger its protection mechanisms, and, in extreme scenarios, even cause cascading failures across transmission-scale systems.[60]

Grid-Enhancing Technologies

Though grid-enhancing technologies (GETs)—hardware and software solutions aimed at optimizing power lines—are not yet widespread in the United States, select utilities are piloting them to extract more capacity from congested power lines, strained by insufficient transmission and distribution infrastructure.[61] The grid's limits are clashing with a wave of power demand from data centers, manufacturing, and electrification, as well as new generation sources.[62] Given current bottlenecks, GETs, such as power flow controllers that redirect electricity across the network, shifting it off overloaded lines and onto underutilized corridors, can relieve congestion and increase the capacity of aging infrastructure. As grid pressures intensify, GETs are positioned to become central technologies on the AI-energy frontier, forming the layer of intelligence through which constrained grids can meet new demand. These technologies introduce vulnerabilities of their own, relying on sensors, accurate data, and software to help operators deploy electricity to underutilized power lines.[63]

As detailed above, natural gas supply, LPTs, control systems, facility-level microgrids, and GETs form the energy backbone of U.S. AI capability; they, and the systems on which they depend, are also the very terrain that groups like Russia's Berserk Bear, Salt Typhoon, and Volt Typhoon have spent years mapping.[64]

AI's Poison Arrow: The Attack

To demonstrate how the energy-AI infrastructure nexus can be exploited to degrade U.S. AI services, this section takes the perspective of a state-level threat actor. The Invisible Backbone Series defines threat actors as attackers with three attributes: (1) the intent to inflict harm, (2) the ability to identify a sector's exploitable vulnerabilities, and (3) the capacity to strike selected targets.[65] Though non-state actors could carry out similar attacks, this paper limits its scope to state-level threats, as states are the best-resourced and most capable attackers. The scenario below follows a fictional state-linked actor, Lindworm, with the patience to spend years inside U.S. networks and the resources to act across cyber and physical domains.

To achieve lasting effects, Lindworm first identifies targets where damage would have the broadest impact and be difficult to reverse; where capacity is nearly fully utilized, leaving no buffer to absorb shortfalls; and where failure would affect the AI infrastructure that is most critical to the actor's goals. AI services increasingly underpin U.S. national security operations and government services, so the Lindworm attacker, seeking a military advantage, targets the energy infrastructure chokepoints that power data center clusters supporting classified U.S. defense operations.[66]

Lindworm first maps the electricity systems powering its AI targets by infiltrating peripheral organizations linked to transmission and distribution system operators, employing the same approach Berserk Bear used. This espionage campaign tells the group which substations feed which data center campuses, which pipelines serve which generators, and where a single transformer carries power for many facilities at once.

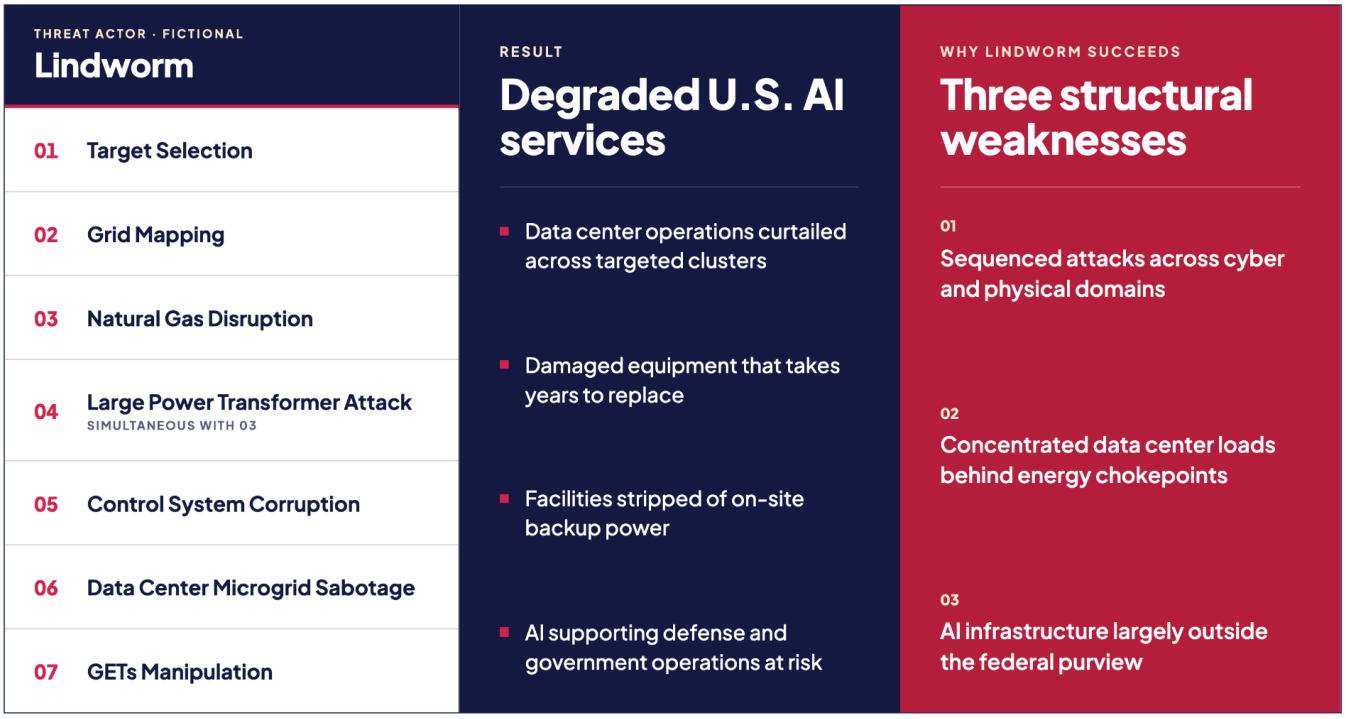
With the map in hand, Lindworm attacks the natural gas pipelines and compressors serving major data center hubs, such as Data Center Alley. Because the same pipelines serve many customers, an attack on U.S. natural gas infrastructure could lead operators to deprioritize data center electricity delivery in favor of powering hospitals or households, curtailing the facilities' grid supply.[67] In a prolonged attack, the targeted data centers' backup fuel reserves could be exhausted, leaving the facilities without on-site redundancy.

Simultaneously, Lindworm targets the LPTs where power losses would be widely felt and slow to repair, attacking the substations that serve concentrated data center loads. The custom-built nature of LPT equipment means transformer spares and interchangeable parts can rarely be quickly substituted.[68] LPT replacement lead times already run for up to five years, but Lindworm extends these by striking upstream manufacturers and electrical steel producers.[69]

The group then corrupts control system data to cause supply-demand imbalances on the grid, leading to instabilities and faults in data center-serving regions. Since data centers tend to be voltage-sensitive, they quickly respond to these grid fluctuations, suddenly and simultaneously dropping large loads off the grid.[70] Meanwhile, operators, working from corrupted feeds and delayed by momentary latency, are too late to respond; others respond to events that never happened.[71] The grid grows more unstable. Lindworm then targets the data centers' microgrids, accessing their controllers to disrupt islanding (the deliberate disconnection from a utility grid) and manipulate automated curtailment signals, sending more loads off the grid.[72] Lindworm also attacks the battery energy storage system controls that provide data centers with backup power,[73] preventing the on-site batteries from discharging.[74] Combined with the generation, transmission, and distribution attacks, the operation strips data centers of their redundancy, curtailing operations. Finally, where GETs are installed, Lindworm targets these by falsifying GET data to push power lines past safe limits, damaging the equipment and interrupting electricity delivery to nearby data centers.[75]

What makes Lindworm particularly troubling is its sequencing and exploitation of vulnerabilities that concentrated data center loads bring to the U.S. energy system. While the U.S. government has institutional structures for securing energy and IT systems, AI infrastructure remains largely outside the federal purview, limiting security coordination.

FIGURE **The Lindworm attack sequence**



A Porous Policy Landscape

In the section above, Lindworm succeeds because it operates in the chasm between two governance regimes, where energy is safeguarded while AI infrastructure is overlooked. This section examines where that chasm lies as a prerequisite for closing it.

Energy is a tightly regulated critical infrastructure (CI) sector, with authorities stemming from statute and executive actions. The U.S. government maintains CI sector security under public-private collaborations,[76] where private CI owners and operators assess and mitigate risks to their own assets, while federal agencies evaluate and manage security on a cross-sector and national level.[77] The Department of Energy (DOE) serves as the Sector Risk Management Agency (SRMA) for energy, and, by statute, it is responsible for (1) "providing institutional knowledge and specialized expertise" to the sector and (2) securing the sector from an "all hazards environment."[78]

The federal government's energy regulatory oversight and CI coordination authorities stem from separate congressional mandates but are mutually reinforcing. For example, under the Federal Power Act, the Federal Energy Regulatory Commission (FERC) approves, and NERC enforces, Critical Infrastructure Protection standards for energy system owners and operators.[79] The Department of Homeland Security's coordination role also allows for quick responses to security issues. Thanks to existing CI coordination mechanisms and regulatory authority, following the Colonial Pipeline attack, the Transportation Security Administration (TSA) was able to issue the first cybersecurity directives to pipeline operators, requiring them to disclose cybersecurity incidents, appoint a Cybersecurity Coordinator, and submit risk assessment results to CISA and the TSA.[80]

AI infrastructure, however, sits outside this architecture, addressed only by fragmented efforts originating in the energy sector. AI is not a designated sector, and, until recently, data centers were treated as ordinary customers on the grid's distribution side. But the status quo is shifting. On July 16, 2026, FERC directed NERC to file mandatory reliability standards and registration criteria for computational loads by the end of the year.[81] In addition, DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is launching an Artificial Intelligence for Operationally Resilient Technologies and Systems (AI-FORTS) program to expand AI-enabled technologies for energy security.[82] Meanwhile, the Cyber Incident Reporting for Critical Infrastructure Act, which aims to give the federal government a cross-sector view of security incidents, has been in rulemaking for over two years without a final rule as of writing.[83] This leaves a porous policy landscape that fails to account for the unique vulnerabilities that the energy-AI nexus brings.

Recommendations

The energy-AI infrastructure attack surface is expanding. Threats to the sectors are both kinetic and cyber; key assets are vulnerable to both; and behind-the-meter generation, storage, and control systems are now adding new adversary entry points. Meanwhile, PRC- and Russia-backed operators have already mapped U.S. critical infrastructure networks. Faced with these threats, the United States must identify and mitigate harm across an expanding attack surface that can be used to disrupt not only data centers' power systems but also interdependent critical infrastructure.

To better secure energy-AI infrastructure against sophisticated state actors, the U.S. government should take the following four steps:

Designate AI as a Critical Infrastructure Sector

Congress and the President have the authority to designate the AI sector as critical infrastructure, opening a sector-wide public-private coordination mechanism with the AI industry, federal agencies, and interdependent CI sectors.[84] A CI designation would assign an SRMA to the AI sector, allowing the agency to coordinate with the DOE to identify and mitigate interdependent vulnerabilities in the face of new attacks.[85] In addition, the designation would fold AI into the CI ecosystem, subjecting AI infrastructure operators to cyber incident reporting, public-private engagements on national security resilience, federal threat intelligence sharing, and executive intervention to secure essential supply chains.[86]

Set Security Baselines

To ensure AI infrastructure resilience from state-level threats, Congress can grant SRMAs the power to set baseline security standards for particularly vulnerable AI and energy infrastructure entities, such as large power transformers and data center clusters. Under the National Security Memorandum 22 (NSM-22), currently under review,[87] the President directed federal agencies with existing regulatory authorities to "establish minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure."[88] Congress can go beyond NSM-22 to grant SRMAs the statutory authority to set national security baselines for designated CI sectors, allowing these agencies to enforce security and resilience measures for the CI owners and operators most likely to be targeted by state actors.[89]

Mandate Periodic Wargaming for AI-Energy Infrastructure Security

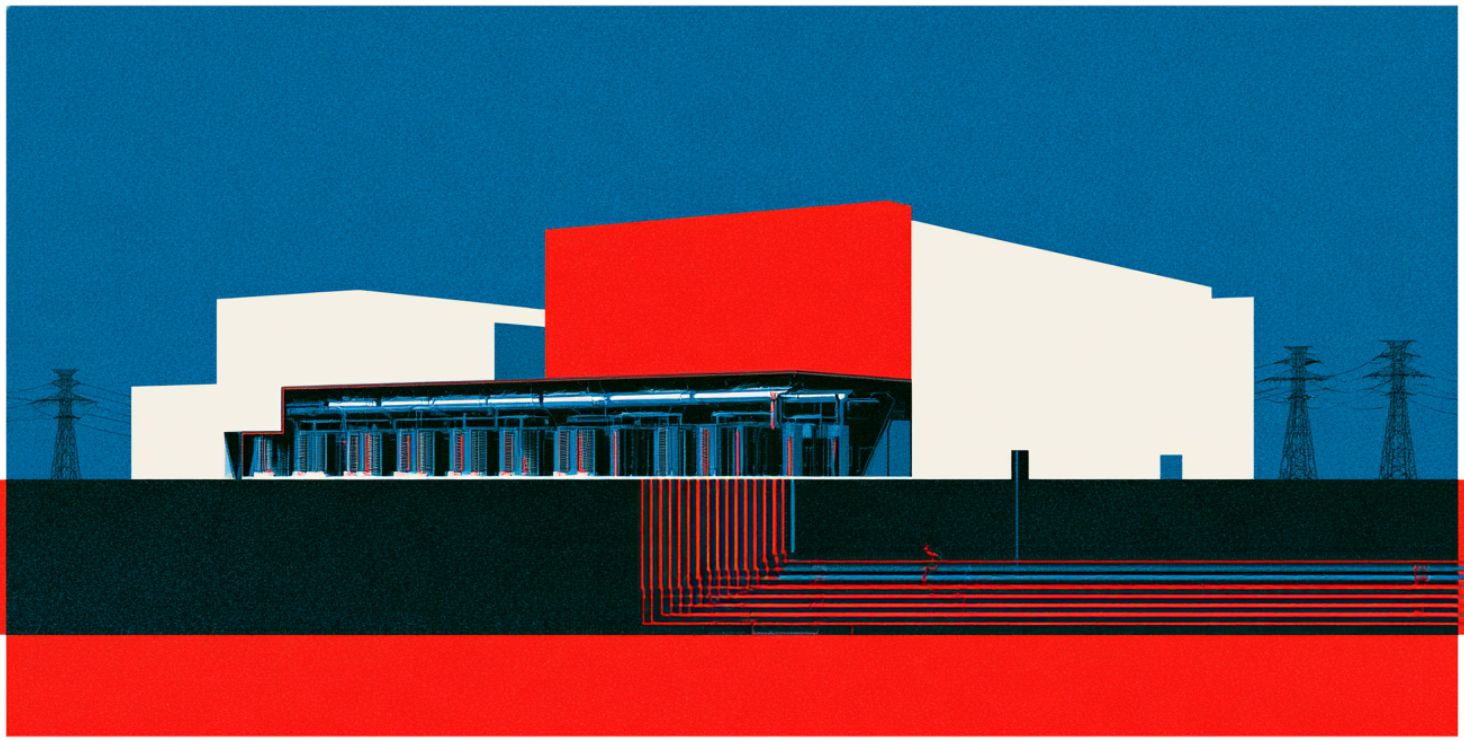
To anticipate threats early, the DOE, supported by the intelligence community, should coordinate with NERC and the AI SRMA to run tabletop and live exercises (i.e., wargames) that assess the threats that capable actors pose to AI and energy infrastructure security. These exercises would improve cross-sector threat detection and response, produce well-defined security metrics, and establish clear communication protocols across the AI and energy sectors.

Set Large-Load Reliability Standards

Following FERC's recent direction, NERC should include standards that safeguard the energy-AI infrastructure nexus from cyber and physical security threats. NERC can also require that any control systems and GETs that utilities and data center operators deploy onto grids serving data center clusters be secure by design.

Conclusion

U.S. AI capabilities rest on an energy system that state actors have already spent over a decade navigating. That system was aging before AI juggernauts' demand arrived at gigawatt scale. The demand is here, and data centers are introducing a new class of vulnerabilities. The fastest-growing loads in the country now sit at the end of chokepoints that adversaries already understand. Berserk Bear mapped energy systems to learn which switch to flip. Volt Typhoon pre-positioned software for activation in future conflicts. As the grid is being transformed by new energy demand, generation, and technology, the U.S. government has an obligation to ensure that these systems incorporate safety standards that are tailored to the threats that AI infrastructure concentrates and exacerbates.



Acknowledgements & Contributions

This research is the product of months of research. ARI acknowledges the following individuals for their contributions to its final form and substance:

Author:

Jess Maksimov, Policy Analyst

Contributors:

Terrence Kelly, PhD*
Elena Berger, PhD

*For additional work published by Terrence Kelly, please see his Substack: In Plain Sight

Endnotes

[1] Terrence Kelly and Jess Maksimov, *The Invisible Backbone: How to Secure AI Infrastructure Today for Tomorrow* (Americans for Responsible Innovation, 2026), https://ari.us/wp-content/uploads/2026/08/ARI_AI_Backbone_Report_080626.pdf.

[2] International Energy Agency, *Energy and AI* (IEA, 2025), https://www.iea.org/reports/energy-and-ai; Electric Power Research Institute, *Powering Intelligence 2026: Updated Scenarios of U.S. Data Center Electricity Use and Power Strategies*, 3002034696 (Electric Power Research Institute, 2026), https://www.epri.com/research/products/000000003002034696.

[3] U.S. Department of Energy, "Addressing Security and Reliability Concerns of Large Power Transformers," Department of Energy, accessed September 29, 2026, https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers.

[4] Andy Greenberg, "The Russian Hackers Playing 'Chekhov's Gun' with US Infrastructure," *Wired*, October 26, 2020, https://www.wired.com/story/berserk-bear-russia-infrastructure-hacking/.

[5] Symantec Threat Hunter Team, "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group," Broadcom, October 20, 2017, https://www.security.com/threat-intelligence/dragonfly-energy-sector-cyber-attacks; U.S. Cybersecurity and Infrastructure Security Agency, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," CISA, Alert TA18-074A, March 16, 2018, https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors; Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110; Rebecca Smith, "How a U.S. Utility Got Hacked," *Wall Street Journal*, December 30, 2016, https://www.wsj.com/articles/how-a-u-s-utility-got-hacked-1483120856.

[6] Andy Greenberg, "Hackers Gain Switch-Flipping Access to US Power Systems," *Wired*, September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

[7] Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," CISA, Cybersecurity Advisory AA24-038A, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[8] Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, IF12798 (Congressional Research Service, 2025), https://www.congress.gov/crs-product/IF12798; CISA, NSA, and FBI, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure"; Sarah Krouse et al., "U.S. Wiretap Systems Targeted in China-Linked Hack," *Wall Street Journal*, October 5, 2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

[9] U.S. Cybersecurity and Infrastructure Security Agency, "Pipeline Cybersecurity," CISA, accessed August 7, 2026, https://www.cisa.gov/resources-tools/programs/pipeline-cybersecurity.

[10] Kelly and Maksimov, *The Invisible Backbone*.

[11] North American Electric Reliability Corporation, *Incident Review: Considering Simultaneous Voltage-Sensitive Load Reductions* (NERC, January 8, 2025), https://www.nerc.com/globalassets/our-work/reports/event-reports/incident_review_large_load_loss.pdf.

[12] Noman Bashir, Rob Sherwood, Le Xie, and Minlan Yu, "From Barrier to Bridge: The Case for AI Data Center/Power Grid Co-Design," arXiv, May 4, 2026, https://doi.org/10.48550/arXiv.2605.03090; North American Electric Reliability Corporation, *Characteristics and Risks of Emerging Large Loads: Large Loads Task Force White Paper* (NERC, 2025), https://www.nerc.com/globalassets/who-we-are/standing-committees/rstc/whitepaper-characteristics-and-risks-of-emerging-large-loads.pdf.

[13] Greenberg, "Russian Hackers Playing 'Chekhov's Gun'"; CISA, "Russian Government Cyber Activity"; Smith, "Russian Hackers Reach U.S. Utility Control Rooms."

[14] Olatunji Ahmed Lawal and Jiashen Teh, "A Framework for Modelling the Reliability of Dynamic Line Rating Operations in a Cyber–Physical Power System Network," *Sustainable Energy, Grids and Networks* 35 (2023): 101140, https://doi.org/10.1016/j.segan.2023.101140; Olatunji Ahmed Lawal et al., "Data-Driven Learning-Based Classification Model for Mitigating False Data Injection Attacks on Dynamic Line Rating Systems," *Sustainable Energy, Grids and Networks* 38 (2024): 101347, https://doi.org/10.1016/j.segan.2024.101347; Ampacimon, "Securing the Smart Grid: Addressing Cybersecurity Challenges in Dynamic Line Rating," February 28, 2025, https://www.ampacimon.com/news/securing-the-smart-grid-addressing-cybersecurity-challenges-in-dynamic-line-rating; Sen Tan et al., "Developments, Challenges and Future Opportunities in Cybersecure Microgrid Control," *Nature Reviews Electrical Engineering* 2 (2025): 522–40, https://www.nature.com/articles/s44287-025-00189-z.

[15] Kelly and Maksimov, *The Invisible Backbone*.

[16] This statistic uses the megawatt figure cited in a 2026 Congressional Research Service report and applies it to gigawatts. According to the report the authors based their figure on an assumption of "a continuous source of electric power generation equal to 100 megawatts (MW), operating year-round, and that the average U.S. household consumes 10,566 kilowatt-hours (kWh) of electricity per year." See Ashley Lawson et al., *Data Centers and Their Energy Consumption: Frequently Asked Questions*, CRS Report R48646 (Congressional Research Service, updated May 12, 2026), https://www.congress.gov/crs-product/R48646; Luis Fernando Enriquez-Contreras et al., *MegaWatt Mayhem: Grid Operator Challenges with Large Loads—Existing Landscape and Grid Stability Implications*, INL/RPT-25-87430 (Idaho Falls, ID: Idaho National Laboratory, September 2025),

https://csdet.inl.gov/content/uploads/45/2025/10/MegaWatt_Mayhem.pdf; Bashir et al., "From Barrier to Bridge"; U.S. Department of Energy, Office of Nuclear Energy, *The Ultimate Fast Facts Guide to Nuclear Energy* (DOE, February 2024), https://www.energy.gov/sites/default/files/2024-02/ne-2023fastfactsguide-021424.pdf.

[17] Peter Fitzmaurice et al., *Characterizing Large Loads: A Taxonomy to Support Large Load Integration*, INL/RPT-25-88356 (Idaho Falls, ID: Idaho National Laboratory, 2025), https://inl.gov/content/uploads/2023/07/Characterizing-Large-Loads-A-Taxonomy-to-Support-Large-Load-Integration.pdf; Lawson et al., *Data Centers and Their Energy Consumption*.

[18] Fitzmaurice et al., *Characterizing Large Loads*; Lawson et al., *Data Centers and Their Energy Consumption*; Venkat Somala and Ben Cottier, "Build times for gigawatt-scale data centers can be 2 years or less," EpochAI, November 10, 2025, https://epoch.ai/data-insights/data-centers-buildout-speeds.

[19] The area has over 250 data centers, with more developments on the way. See Northern Virginia Regional Commission, "Data Centers," 2026, https://www.novaregion.org/1598/Data-Centers; Ben Levitt and Doug Giuffre, "Navigating US Data Center Energy Demand," S&P Global, December 2, 2025, https://www.spglobal.com/en/research-insights/special-reports/look-forward/data-center-frontiers/navigating-us-data-center-energy-demand.

[20] IEA, *Energy and AI*; Xin Chen et al., "Electricity Demand and Grid Impacts of AI Data Centers: Challenges and Prospects," arXiv:2509.07218, August 4, 2026, https://arxiv.org/abs/2509.07218.

[21] IEA, *Energy and AI*; EPRI, *Powering Intelligence 2026*.

[22] IEA, *Energy and AI*.

[23] S&P Global also finds that as states and regulators increasingly implement data center load reliability standards, on-site redundancy will likely rely on gas-powered technologies more than any other source. See Brian Martucci, "Texas Law Gives Grid Operator Power to Disconnect Data Centers During Crisis," *Utility Dive*, June 25, 2025, https://www.utilitydive.com/news/texas-law-gives-grid-operator-power-to-disconnect-data-centers-during-crisi/751587/; Levitt and Giuffre, "Navigating US Data Center Energy Demand"; IEA, *Key Questions on Energy and AI* (IEA, April 2026), https://www.iea.org/reports/key-questions-on-energy-and-ai.

[24] North American Electric Reliability Corporation, *2025 ERO Reliability Risk Priorities Report*, NERC, July 22, 2025, https://www.nerc.com/globalassets/our-work/reports/ero-reliability-risk-priorities-report/2025_risc_ero_priorities_report.pdf.

[25] Ibid.

[26] Dennis Romero, "Cyberattack Forces Colonial Pipeline to Shut Major Fuel Line," *NBC News*, May 8, 2021, https://www.nbcnews.com/news/us-news/cyberattack-forces-colonial-pipeline-shut-major-fuel-line-n1266737.

[27] Joseph Menn and Stephanie Kelly, "Colonial Pipeline slowly restarts as Southeast U.S. scrambles for fuel," *Reuters*, May 12, 2021, https://www.reuters.com/business/energy/top-us-fuel-pipeline-edges-toward-reopening-gasoline-shortages-worsen-2021-05-12/; Jeff St. John, "The Colonial Pipeline Ransomware Shutdown: A Wake-Up Call for Energy Cybersecurity," *Canary Media*, May 11, 2021, https://www.canarymedia.com/articles/fossil-fuels/colonial-pipeline-shutdown-a-wakeup-call-for-energy-cybersecurity.

[28] CISA, "Pipeline Cybersecurity."

[29] Ibid.

[30] U.S. Cybersecurity and Infrastructure Security Agency, "Ransomware Impacting Pipeline Operations," CISA, October 24, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-049a.

[31] Paul W. Parfomak, *Pipeline Physical Security: Federal Efforts*, CRS Insight IN12161 (Congressional Research Service, May 11, 2023), https://www.congress.gov/crs-product/IN12161.

[32] Parfomak, *Pipeline Physical Security*; U.S. Attorney's Office, Southern District of Iowa, "Arizona Woman Sentenced to Six Years in Prison for Conspiracy to Damage the Dakota Access Pipeline," September 23, 2022, https://www.justice.gov/usao-sdia/pr/arizona-woman-sentenced-six-years-prison-conspiracy-damage-dakota-access-pipeline.

[33] DOE, "Addressing Security and Reliability Concerns of Large Power Transformers"; Yuhao Huang et al., "Artificial Intelligence Data Centers and Power System Sustainability: Understanding the Sustainability Implications of AI-Driven Data Centers on Power Systems," *IEEE Energy Sustainability Magazine* 2, no. 3 (August 2026): 41–55, https://doi.org/10.1109/ESM.2026.3676745; DataBank, "A Closer Look at DataBank's Salt Lake City Substation," February 1, 2022, https://www.databank.com/resources/blogs/unveiling-databanks-new-salt-lake-city-substation/; Enercon, "Data Center Power Fundamentals," accessed August 7, 2026, https://www.enercon.com/data-center-power-fundamentals/; Business Wire, "Data Center Transformers Industry Analysis Report 2025: Growth in Hyperscale and Mega Data Centers Drives Demand for High-Efficiency, High-Capacity Power Transformers—Global Market Forecast to 2030," *Business Wire*, November 11, 2025, https://www.businesswire.com/news/home/20251111769332/en/Data-Center-Transformers-Industry-Analysis-Report-2025-Growth-in-Hyperscale-and-Mega-Data-Centers-Drives-Demand-for-High-Efficiency-High-Capacity-Power-Transformers---Global-Market-Forecast-to-2030---ResearchAndMarkets.com; Flex-Core, "Using Current and Voltage Transformers in Data Centers," December 2019, https://www.flex-core.com/engineering-resources/application-whitepapers/using-current-and-voltage-transformers-in-data-centers/; Occupational Safety and Health Administration, "Substations," Illustrated Glossary, accessed August 7, 2026, https://www.osha.gov/etools/electric-power/illustrated-glossary/sub-station.

[34] DOE, "Addressing Security and Reliability Concerns of Large Power Transformers."

[35] National Infrastructure Advisory Council, *Addressing the Critical Shortage of Power Transformers to Ensure Reliability of the U.S. Grid* (Cybersecurity and Infrastructure Security Agency, June 11, 2024), https://www.cisa.gov/sites/default/files/2024-09/NIAC_Addressing%20the%20Critical%20Shortage%20of%20Power%20Transformers%20to%20Ensure%20Reliability%20of%20the%20U.S.%20Grid_Report_06112024_508c_pdf_0.pdf.

[36] Ibid.

[37] Paul W. Parfomak, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, CRS Report R43604 (Congressional Research Service, July 2, 2015), https://www.congress.gov/crs-product/R43604.

[38] Eyder Peralta, "Sniper Attack on Calif. Power Station Raises Terrorism Fears," *NPR*, February 5, 2014, https://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears.

[39] Kennedy Maize, "Grid Security Gets Physical," *POWER*, August 1, 2014, https://www.powermag.com/grid-security-gets-physical/.

[40] Paul W. Parfomak, *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?*, CRS Report R45135 (Congressional Research Service, March 19, 2018), https://www.congress.gov/crs-product/R45135.

[41] Christopher Cox, "What if America Went Completely Dark?," *New York Times Magazine*, August 18, 2026, https://www.nytimes.com/2026/08/18/magazine/national-blackout-power-electricity-outage.html.

[42] Steve Almasy et al., "Power may be back for thousands on Wednesday night as authorities continue to go through tips on electric substation attack," *CNN*, December 7, 2022, https://www.cnn.com/2022/12/06/us/power-outage-moore-county-investigation-tuesday/index.html; Federal Bureau of Investigation, "Shooting of Electrical Substations," FBI, December 3, 2022, https://www.fbi.gov/wanted/seeking-info/shooting-of-electrical-substations.

[43] NERC, *2025 ERO Reliability Risk Priorities Report*.

[44] Fitzmaurice et al., *Characterizing Large Loads*.

[45] Enriquez-Contreras et al., *MegaWatt Mayhem*.

[46] Americans for Responsible Innovation, "Behind the Build: Grid Mitigation & Data Centers," ARI, June 2026, https://datacenterplaybook.org/playbook.html.

[47] An inflexible load is "unable to adjust power consumption quickly for purposes of ancillary services due to resultant operational impacts. This inability can be driven by factors such as lack of on-site storage or generation, lack of grid communications capability, mission criticality, and/or organizational rules and policies." See Fitzmaurice et al., *Characterizing Large Loads*.

[48] Enriquez-Contreras et al., *MegaWatt Mayhem*.

[49] Claire Gauthier et al., *AI Meets the Grid Shaping the Data Centers*, Capgemini Research Institute, June 2026. https://www.capgemini.com/wp-content/uploads/2026/06/CRI_Data-centers_V10_interactive.pdf; Ketchum & Walton Co., "What Is the Cost of Data Center Downtime & How to Prevent It," September 12, 2025, https://ketchumandwalton.com/what-is-the-cost-of-data-center-downtime-how-to-prevent-it/.

[50] Data centers often use uninterruptible power supply (UPS) systems that can instantaneously provide electricity to the facility in the event of a grid outage. Some facilities also use protection schemes that automatically transfer data center load to a backup system after a set number of disturbances; the facility then remains off the grid until operators manually reconnect it. See NERC, *Incident Review*.

[51] Tim McLaughlin, "Big Tech's data center boom poses new risk to US grid operators," *Reuters*, March 19, 2025, https://www.reuters.com/technology/big-techs-data-center-boom-poses-new-risk-us-grid-operators-2025-03-19/; NERC, *Incident Review: Considering Simultaneous Voltage-Sensitive Load Reductions*; NERC, *Characteristics and Risks of Emerging Large Loads*; North American Electric Reliability Corporation, *Standards and Compliance Bulletin* (NERC, January 20, 2026), https://www.nerc.com/globalassets/who-we-are/news/2026/01/2026_1_20_standardscompliancebulletin.pdf; Rachel Mural et al., *AI, Data Centers, and the U.S. Electric Grid: A Watershed Moment* (Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2026), https://www.belfercenter.org/research-analysis/ai-data-centers-us-electric-grid.

[52] Enriquez-Contreras et al., *MegaWatt Mayhem*; Alexander Anderson et al., *Transmission Operator Workflows for Real-Time Reliability Studies: A Review of Control Room Practices and Naturalistic Decision Making*, PNNL-36516 (Pacific Northwest National Laboratory, 2024), https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-36516.pdf; R.W. Hurst, "What Is SCADA?," The Electricity Forum, accessed August 7, 2026, https://electricityforum.com/td/smart-grid/what-is-scada.

[53] Kyle Thomas et al., "Practical Guidance and Considerations for Large Load Interconnections" (presentation slides, September 18, 2025), https://www.in.gov/dA/cc6b7235a6/4.-Practical-Guidance-and-Considerations-for-Large-Load-Interconnections.pdf?language_id=1.

[54] NERC, *2025 ERO Reliability Risk Priorities Report*.

[55] NERC, *2025 ERO Reliability Risk Priorities Report*; Greenberg, "Russian Hackers Playing 'Chekhov's Gun.'"

[56] Gauthier et al., *AI Meets the Grid Shaping the Data Centers*.

[57] The Department of Energy defines a microgrid as "a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. It can connect and disconnect from the grid

to enable it to operate in grid-connected or island-mode." See Dan Ton, "Microgrid R&D Program at the U.S. DOE," (presentation slides, November 2018), https://www.energy.gov/documents/remote-microgrids-dan-tonpdf; Enriquez-Contreras et al., *MegaWatt Mayhem*; Weintek USA, "Every Place an HMI Lives Inside a Data Center—and Why It Matters for Your Next Build," April 6, 2026, https://www.weintekusa.com/every-place-an-hmi-lives-inside-a-data-center-and-why-it-matters-for-your-next-build/; Chris Murphy, "6 Insights on How Complex Microgrids Support Data Center Power Strategy," *Data Center World*, accessed August 7, 2026, https://datacenterworld.com/article/6-insights-on-how-complex-microgrids-support-data-center-power-strategy/.

[58] Gauthier et al., *AI Meets the Grid Shaping the Data Centers.*

[59] Ibid.

[60] Zhouhao Ji et al., "Bit2Watt: A Cyber-Physical Vulnerability Exploiting GPU Workloads across Power and Computing Infrastructures," arXiv, July 7, 2026, https://doi.org/10.48550/arXiv.2607.05993.

[61] National Conference of State Legislatures, "Grid Enhancing Technologies," NCSL, October 24, 2025, https://www.ncsl.org/energy/grid-enhancing-technologies; Eduardo Garcia, "US Utilities Scale Up Grid-Boosting Tech to Meet Surging Demand," *Reuters*, March 9, 2026, https://www.reuters.com/business/energy/us-utilities-scale-up-grid-boosting-tech-meet-surging-demand--reeii-2026-03-09/; U.S. Department of Energy, Office of Electricity, "Grid-Enhancing Technologies: From Research and Development to Reality," October 20, 2023, https://www.energy.gov/oe/articles/grid-enhancing-technologies-research-and-development-reality; Idaho National Laboratory, *A Guide to Case Studies for Grid-Enhancing Technologies* (INL, 2023), https://inl.gov/content/uploads/2023/03/A-Guide-to-Case-Studies-for-Grid-Enhancing-Technologies.pdf.

[62] NERC, *2025 ERO Reliability Risk Priorities Report.*

[63] U.S. Department of Energy, Office of Electricity, "Grid-Enhancing Technologies Improve Existing Power Lines," accessed August 7, 2026, https://www.energy.gov/oe/grid-enhancing-technologies-improve-existing-power-lines; U.S. Department of Energy, *Grid-Enhancing Technologies: A Case Study on Ratepayer Impact* (DOE, February 2022), https://www.energy.gov/sites/default/files/2022-04/Grid%20Enhancing%20Technologies%20-%20A%20Case%20Study%20on%20Ratepayer%20Impact%20-%20February%202022%20CLEAN%20as%20of%20032322.pdf.

[64] Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*; Andy Greenberg, "The Russian Hackers Playing 'Chekhov's Gun' with US Infrastructure"; CISA, NSA, and FBI, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure."

[65] Kelly and Maksimov, *The Invisible Backbone.*

[66] Ibid.

[67] PJM Legislators Collaborative, "State elected official coalition letter to PJM," November 17, 2025, https://www.pjm.com/-/media/DotCom/about-pjm/who-we-are/public-disclosures/2025/20251118-pjm-legislators-collaborative-letter-re-cifp-lla.pdf.

[68] Cox, "What if America Went Completely Dark?"

[69] U.S. Department of Energy, *Large Power Transformer Resilience* (DOE, July 2024), https://www.energy.gov/sites/default/files/2024-10/EXEC-2022-001242%20-%20Large%20Power%20Transformer%20Resilience%20Report%20signed%20by%20Secretary%20Granholm%20on%207-10-24.pdf.

[70] NERC, *Incident Review.*

[71] William Conklin, "How Does SCADA Work?," Electricity Forum, accessed August 7, 2026, https://electricityforum.com/td/smart-grid/how-does-scada-work.

[72] NERC, *Incident Review.*

[73] Frans Öhrström et al., "From Balance to Breach: Cyber Threats to Battery Energy Storage Systems," *Energy Informatics* 8, no. 1 (2025): article 39, https://doi.org/10.1186/s42162-025-00499-4; Enriquez-Contreras et al., *MegaWatt Mayhem.*

[74] "Any interruption, whether due to grid faults, voltage sags, or planned outages, can result in data loss, service-level agreement (SLA) violations, or financial penalties." See Enriquez-Contreras et al., *MegaWatt Mayhem.*

[75] Tan et al., "Developments, Challenges and Future Opportunities in Cybersecure Microgrid Control"; Lawal and Teh, "A Framework for Modelling the Reliability of Dynamic Line Rating Operations"; Lawal et al., "Data-Driven Learning-Based Classification Model for Mitigating False Data Injection Attacks on Dynamic Line Rating Systems"; Ampacimon, "Securing the Smart Grid."

[76] Brian E. Humphreys, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, CRS Report R48878 (Congressional Research Service, March 10, 2026), 3, https://www.congress.gov/crs-product/R48878.

[77] Ibid.

[78] See Humphreys, *Critical Infrastructure;* Definitions, 6 U.S.C. § 650(23), https://www.law.cornell.edu/uscode/text/6/650.

[79] Federal Energy Regulatory Commission, "Cyber and Grid Security," FERC, December 12, 2023, https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security.

[80] Humphreys, *Critical Infrastructure*; Parfomak, *Pipeline Physical Security.*

[81] Federal Energy Regulatory Commission, "Order Directing the North American Electric Reliability Corporation to File Reliability Standard(s) Pertaining to Computational Load Integration," Docket No. RD26-7-000, July 16, 2026, https://www.ferc.gov/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.ferc.gov%2Fsites%2Fdefault%2Ffiles%2F2026-07%2FRD26-7-000.pdf.

[82] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *CESER Strategic Plan: Fiscal Years 2026 to 2030* (U.S. Department of Energy, 2026), https://www.energy.gov/documents/ceser-strategic-plan2026-2030.

[83] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 1038; https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements; Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) (to be codified at 6 C.F.R. pt. 226), https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

[84] Sector Risk Management Agencies, 6 U.S.C. § 652a, https://www.law.cornell.edu/uscode/text/6/652a.

[85] Brian E. Humphreys, *The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience* (Congressional Research Service, 2024), https://www.congress.gov/crs-product/IF12716; Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c, https://www.law.cornell.edu/uscode/text/42/5195c; U.S. Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," CISA, accessed June 22, 2026, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors; Crowell & Moring, "Changes to Critical Infrastructure Requirements," Crowell, January 28, 2025, https://www.crowell.com/en/insights/publications/changes-to-critical-infrastructure-requirements; Megan Brown et al., "New White House Policy Previews Increased Cybersecurity Oversight and Regulation," Wiley Rein LLP, May 2, 2024, https://www.wiley.law/alert-New-White-House-Policy-Previews-Increased-Cybersecurity-Oversight-and-Regulation.

[86] Asad Ramzanali, *How to Regulate the Cloud: A Blueprint to Address the Market Failures and National Security Risks of Cloud Computing* (Vanderbilt Policy Accelerator, 2025), https://doi.org/10.2139/ssrn.6222822.

[87] Caitlin Clarke and Andy Kotz, "Trump EO Aims to Streamline Critical Infrastructure Resilience," Center for Cybersecurity Policy and Law, March 19, 2025, https://www.centerforcybersecuritypolicy.org/insights-and-research/trump-eo-aims-to-streamline-critical-infrastructure-resilience.

[88] Joseph R. Biden, "National Security Memorandum on Critical Infrastructure Security and Resilience," The American Presidency Project, April 30, 2024, https://www.presidency.ucsb.edu/documents/national-security-memorandum-critical-infrastructure-security-and-resilience.

[89] Ibid.