DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

Securing Grid Communications Infrastructure: Addressing Gaps Beyond NERC CIP Facility Perimeters

Digital Assurance Brief #1

OCTOBER 2025

INL/RPT-25-89588

Center for Securing Digital Energy Technology

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

INL/RPT-25-89588

Securing Grid Communications Infrastructure: Addressing Gaps Beyond NERC CIP Facility Perimeters

Digital Assurance Brief #1

OCTOBER 2025

Idaho National Laboratory
National & Homeland Security
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CONTENTS

ACRONYMS

ADMS	Advanced Distribution Management System
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
BES	Bulk Electric System
CIP	Critical Infrastructure Protection
DERMS	Distributed Energy Resource Management System
DOE	U.S. Department of Energy
EAP	Electronic Access Point
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
GIS	Geographic Information System
NERC	North American Electric Reliability Corporation
PRC	People's Republic of China
SCADA	Supervisory Control and Data Acquisition
U.S.	United States

Securing Grid Communications Infrastructure: Addressing Gaps Beyond NERC CIP Facility Perimeters

Digital Assurance Brief #1

1. Executive Summary

The North American electric grid faces a significant cybersecurity gap that poses a threat to its reliability and resilience. While the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards provide security requirements for equipment within facility perimeters, all communications infrastructure beyond Electronic Access Points (EAPs) remains largely unregulated. This includes, for example, communications between control centers and substations or between control centers and generation plants. These critical circuits are outside the Electronic Security Perimeter (ESP) and not covered by mandatory federal requirements. This exemption creates exposure that adversaries can exploit through unencrypted protocols, compromised supply chains, and unsecured field communications.

This regulatory gap becomes more problematic as the grid's communication landscape evolves. Dispatchable generation and storage assets and load control, advanced metering infrastructure (AMI), and distribution system edge devices are proliferating across the grid, often falling below federal regulatory risk thresholds. The associated communications may integrate into traditional architectures through existing protected utility infrastructure, but many also connect to external sources such as manufacturers, integrators, or cloud storage providers, further expanding the attack surface beyond regulatory oversight.

Many of the systems that provide critical communications among these burgeoning segments of the modern grid, and that facilitate their operation as part of the larger grid, still rely on channels somewhere in the architecture that transmit data in clear text without encryption. Meanwhile, critical assets of grid communications, such as routers, modems, and network devices, increasingly contain components from foreign manufacturers with documented security vulnerabilities. Most assets include at least one subcomponent from China.

The magnitude of grid communications risks is increasingly top-of-mind, as Chinese state-sponsored advanced persistent threats (APTs), including Volt Typhoon, Salt Typhoon, and Flax Typhoon, actively target this infrastructure. In June 2025, the Department of Energy's (DOE's) Electricity Advisory Committee concluded that reliance on third-party telecommunications providers creates what industry calls a "black box risk," noting that the People's Republic of China (PRC's) Salt Typhoon campaign poses a "severe and continuing challenge" to U.S. telecommunications systems on which many utilities depend.[1] The Committee emphasized that the PRC and Russia have demonstrated both the intent and capability to target telecommunications infrastructure, with the PRC's interest in causing societal impact aligning directly with systemic risk to the Bulk Electric System (BES).[1] Other recent threat assessments from inside the United States (U.S.) government have reinforced concerns that adversaries possess both the technical capability and strategic intent to exploit telecommunications access as a pathway to compromise grid operations.

NERC-registered entities are generally dependent on third-party telecom providers for grid communications infrastructure that often contains persistent remote access connections and increasingly relies on cloud-based services. These dependencies fall outside the jurisdiction of NERC CIP, creating a significant regulatory gap in which critical operational communications traverse networks with inconsistent security oversight and unknown threat exposure.

While the technical solution is relatively straightforward—encrypt and authenticate grid communications and physically protect the communication devices—implementing it requires buy-in from stakeholders across the utility landscape, including manufacturers, developers, integrators, aggregators, and utilities. Each stakeholder may have different regulatory or financial incentives, creating complexity for driving secure operational communications for all grid assets that affect reliability. This policy brief examines:

- The scope and drivers of the grid communications exemption and the major categories of risk outside NERC CIP scope.
- Real-world attack vectors where adversaries exploit vulnerable networking equipment, legacy protocols, opaque supply chains, and persistent remote access.
- Structural limitations in the current regulatory framework and why grid modernization accelerates communications risk.
- Practical, near-term recommendations that utilities can implement now, without waiting for new standards, to secure critical communications infrastructure and reduce systemic risk.

Closing this gap will require both proactive utility action and complementary policy evolution so that secure communications become a baseline expectation for all grid-relevant assets, not just those inside facility perimeters.

2. The Communications Security Gap

2.1. Scope of the Grid Communications Exemption

NERC CIP standards comprehensively regulate cybersecurity within facility boundaries but explicitly exempt all grid communications equipment and infrastructure beyond the ESP. This means that routers, modems, circuits, and communications used for control and monitoring of grid assets carrying critical operational data are not required to meet any current NERC CIP compliance requirements.

The exemption originated from practical concerns in the early 2000s when utilities relied on third-party leased lines for communications. Regulators hesitated to impose security requirements on telecommunications providers outside Federal Energy Regulatory Commission (FERC) jurisdiction. However, this regulatory compromise created a permanent gap that becomes more impactful as grid modernization proceeds. There are five major categories of communication security gaps outside of NERC CIP scope:

1. **Control center to facility communications**, including connections between control centers and generation plants or substations, which fall outside the protection of CIP-012 or any other CIP Standard.
2. **Dispatchable distribution-level generation and storage control signals**, many still transmitted over public internet, corporate networks, or cellular networks, with limited or no security safeguards.
3. **Inter-substation communications**, such as supervisory control and data acquisition (SCADA) network traffic which are often reliant on legacy protocols lacking encryption or authentication. While NERC approved CIP-015 Cyber Security—Internal Network Security Monitoring, which mandates internal network monitoring, the enforcement of this standard has been pushed out until 10/1/2028.
4. **Distribution automation signals**, involving smart grid devices and controllers that operate across unregulated communications channels. Distribution systems fall outside NERC CIP's Bulk Electric System (BES) definition; yet the growth in aggregations of small, distributed generators

and automated coordination creates reliability interdependencies that current regulatory frameworks do not address but could nonetheless impact the bulk system.

5. **Third-party communications infrastructure**, including leased circuits and telecommunications provider networks that carry grid operational data but fall outside utility operational control and NERC CIP jurisdiction. These critical pathways often contain persistent remote access connections and increasingly rely on cloud-based services, yet regulators have historically hesitated to impose security requirements on telecommunications providers outside FERC authority.

2.2. Real World Attack Vectors

Recent incidents and intelligence assessments demonstrate that adversaries are actively exploiting these vulnerabilities in grid communications systems through multiple risk channels: exploitation of system vulnerabilities in telecommunications infrastructure and networking equipment; continued reliance on low-security industrial protocols widely deployed across the grid; supply chain compromise of communications equipment; and legitimate, persistent remote access.

Across these incidents, several consistent trends emerge in the exploitation of network-edge devices. Adversaries repeatedly exploit vulnerabilities at trust boundaries where firewalls, VPNs, and routing infrastructure provide broad visibility and authority over internal environments.[2] Exploitation often occurs rapidly after disclosure, relies heavily on delayed or missed vendor-issued patches, and increasingly involves chaining older CVEs with newly discovered zero-day vulnerabilities to complicate detection and prioritization. Because these devices are frequently internet-facing and implicitly trusted, weaknesses such as authentication bypasses, misconfigurations, default or hardcoded credentials, and unauthenticated remote code execution provide attackers with disproportionate access relative to the effort required.[3]

Communication networks and networking equipment may be compromised via software vulnerabilities in the equipment itself by external threat actors. Several documented incidents demonstrate operational impacts to utilities resulting from attacks targeting OT networking equipment, such as firewalls. In 2019, the first cyberattack with operational power grid impact in the U.S. occurred, targeting an exposed Cisco firewall with a known vulnerability used by an independent power producer, sPower.[4] The exploit caused the firewalls to reboot repeatedly, which disrupted communications to generation assets in five-minute intervals over a 12-hour period. While generation continued uninterrupted, sPower had limited ability to monitor and dispatch generation assets. The threat actors were not identified, and available evidence suggests the activity was not specifically targeted at sPower. Instead, the attackers appear to have exploited a known vulnerability in an internet-exposed device discovered through opportunistic scanning, highlighting the importance of securing communications infrastructure within defined security perimeters and the operational risk when those controls are absent.

A similar attack vector was observed in 2023 against Zyxel firewalls used by several Danish utilities, when a known critical vulnerability was exploited in coordinated campaigns against multiple organizations.[5] The first wave targeted unpatched devices, compromising at least 11 companies and allowing remote command execution; a second wave, approximately two weeks later, leveraged additional previously undisclosed vulnerabilities (known as zero-days) on similar devices. Because many devices had not yet been patched, response efforts were constrained until vendor fixes could be deployed. Both incidents highlight the importance of patch management to ensure that threat actors cannot use known vulnerabilities as an initial access point into sensitive networks.

Details released in March 2025, revealed that a local utility in Massachusetts, Littleton Electric Light and Water (LELWD), was targeted by a PRC-sponsored APT dubbed Volt Typhoon. Investigators found that the intrusion began in early 2023 when Volt Typhoon gained unauthorized access to LELWD's network through a FortiGate 300D firewall that had missed a critical security update.[6] Attackers exfiltrated Geographic Information System (GIS) data, which contained the spatial layout of energy grid

operations, credentials for electrical substations, and SCADA system documentation.[7],[8] The attackers then positioned themselves adjacent to operational technology by compromising VMware vCenter servers that manage virtualized infrastructure controlling grid assets.[9] Across multiple U.S. utilities, Volt Typhoon extracted Active Directory databases containing every username and password hash in victim organizations, then moved laterally to systems managing substation communications and control center operations.[10] This incident demonstrates how the compromise of networking equipment can be used by adversaries as an access point to pivot into other parts of the network and achieve a wide range of objectives.

Security risks exist not only with networking equipment itself, but also with communications providers on which grid operators rely. In 2022, an attack on Viasat's KA-SAT network in Europe resulted in partial interruption of satellite broadband service across the continent.[11] The attack occurred via malicious firmware updates that were pushed from a compromised management system, which was exploited using a misconfiguration in a Virtual Private Network (VPN) application. By overwriting critical flash memory data, the firmware update pushed from the compromised management system prevented modems from reconnecting to the satellite network after rebooting. The subsequent reboot command caused tens of thousands of modems to drop offline rapidly. Though the attack did not directly target power infrastructure, one of the attack victims, Enercon, had 5,800 wind turbines affected by the attack. It took almost two months to bring all of the turbines back online, as they each required manual intervention to recover, although the turbines continued to produce power during the attack.[12]

While vulnerabilities may be found in communications equipment due to software bugs or design flaws, there is also concern about supply chain security risks for these devices. Recent congressional action, including the 2024 ROUTERS Act, highlights growing concerns about foreign-manufactured network equipment. Security researchers have documented extensive vulnerabilities in equipment from various manufacturers, including hidden backdoors in firmware,[13] hardcoded credentials that cannot be changed,[14] unpatched vulnerabilities persisting for years,[15] and inadequate security update mechanisms that leave equipment exposed even when patches exist.[16] These issues cannot all be fixed with a simple software patch, raising concerns about more systematic flaws that could be exploited by a motivated adversary or nation-state with privileged access to information about devices manufactured in their country.

Beyond the networking equipment, risks also exist in the type of communication protocols used within power system operations. Several common protocols, including DNP3, IEC 61850, and Modbus, are unencrypted and unauthenticated in their standard application, making it easier for motivated adversaries who already have network access to spoof commands. Research demonstrates that attackers can easily intercept MODBUS communications to inject false commands,[17] modify operational data, or conduct denial-of-service attacks.[18] Spoofed commands using weak protocols (IEC 101, IEC 104, IEC 61850, and OPC) were used in Ukraine's 2016 Industroyer attacks, where malware directly communicated with substation controls using these protocols to send "open breaker" commands, causing blackouts in Kyiv, Ukraine.[19] A similar attack was attempted in 2022 using an updated Industroyer malware, focused primarily on IEC-104, but was foiled before adversaries could cause blackouts.[20],[21] Even more recently, Modbus was used as part of the January 2024 FrostyGoop attack, which spoofed commands to temperature controllers, causing over 600 apartment buildings to lose heat for 48 hours in sub-zero temperatures, affecting approximately 100,000 residents in Lviv, Ukraine. The FrostyGoop malware is notable for its use of Modbus, a common protocol in U.S. power systems, but this attack did not target power systems, and the heating system had less boundary protection than most utilities. However, all three of these incidents demonstrate that once an adversary has access to a network, the use of communications protocols without security features creates opportunity for motivated adversaries to directly affect real-world operations.

Utilities also face contractual constraints that create security blind spots outside of NERC CIP's regulatory reach. Industry stakeholders report that distributed load management, monitoring, and

generation asset vendors, and grid communications vendors frequently require persistent remote access and cloud-based monitoring as non-negotiable conditions of equipment warranties and support contracts, with some utilities discovering only after systems become operational that vendors send operational telemetry to external servers. Vendor service-level agreements require 24/7 remote access for things like predictive maintenance (sometimes without clear definition of security controls), while some third-party agreements may mandate cloud connections that cannot be severed even during active cyber incidents without breaching contracts. Because distributed systems typically fall below NERC CIP registration thresholds, no nationwide regulatory framework exists for minimum security standards for these remote access arrangements or data management practices. An example of the potential consequences of this type of access occurred in 2024, when Deye-branded inverters in the United States became operational after a firmware update from the manufacturer.[22] Deye-branded inverters do not hold mandatory safety certifications for operation in the U.S., but some had still been installed. It is believed that the firmware update included code that started checking for the geolocation of the device based on available network information, and, if it discovered it was in an unauthorized location, shut down. While not a malicious cyber event, it demonstrates the direct and consequential impact of direct manufacturer access to devices.

Together, these incidents demonstrate that grid communications risk is not driven by a single failure mode, but by the convergence of vulnerable networking equipment, insecure legacy protocols, opaque supply chains, and persistent external access. Adversaries do not need novel capabilities to create operational risk. In multiple cases, they have relied on known vulnerabilities, standard management interfaces, and trusted vendor access paths to move adjacent to or directly into operational technology environments. From opportunistic exploitation of exposed firewalls to state-sponsored campaigns leveraging missed patches and legitimate remote access, these pathways repeatedly bypass traditional perimeter defenses.

3. Current Regulatory Framework

3.1. Evolution of NERC CIP Standards

The current regulatory structure emerged from crisis. Following the August 2003 Northeast blackout that affected 55 million people, Congress granted FERC authority to oversee mandatory reliability standards. NERC developed the CIP standards between 2005-2008, but communications security has remained contentious.

Early CIP standards improved internal security but did not address external communications. CIP-004 focused on personnel training and access management, CIP-007 on system security through patching, access controls, and logging, and CIP-010 on configuration management and vulnerability assessments. In 2017, CIP-013 added supply chain risk management, requiring utilities to consider vendor and procurement risks. These measures strengthened facility perimeters but left communications equipment and circuits beyond them unprotected.

CIP-012, approved in 2020 and enforced from 2022, marked the first attempt to secure communications through mandating encryption and authentication for data exchanged between control centers. It also mandated the physical protection of communication equipment. While these CIP expansions have improved the security of the grid, there is still more that needs to be addressed. Such items not addressed are data exchanged with other grid elements, such as all generation plants and substations, and thus most grid communications were left outside mandatory protection. The latest standard, CIP-015, will require internal network monitoring, which will help to strengthen the cybersecurity of the equipment within the facilities.

While these CIP expansions have improved grid security, significant gaps remain. Critical areas such as data exchanged with generation plants and substations fall outside mandatory protection requirements, leaving most grid communications vulnerable. Although the latest standard, CIP-015, will mandate internal network monitoring to strengthen facility-level cybersecurity, enforcement remains several years

away. Meanwhile, the electric grid and its supporting communication infrastructure continue to expand rapidly, incorporating new technologies at a pace that outstrips NERC CIP's ability to adapt and provide adequate regulatory coverage.

The pace of NERC CIP evolution itself presents a structural challenge. Standards development follows a multi-year consensus process involving industry stakeholders, NERC committees, and FERC approval, a timeline that struggles to match the rapid deployment of new grid technologies. For example, NERC CIP standards only recently incorporated terminology addressing virtualization technology, despite utilities having deployed virtualized systems for over a decade. Similarly, the growth of distribution automation, grid-edge power production, and storage has outpaced regulatory frameworks designed for traditional bulk power assets. This regulatory lag creates a recurring pattern where utilities deploy new digital technologies years before mandatory security standards exist to govern them, forcing utilities to rely on voluntary best practices or risk-based approaches in the interim.

Closing the gaps in NERC CIP standards is further complicated by jurisdictional fragmentation across multiple regulatory bodies. FERC and NERC regulate the bulk electric system, including communication systems within utility facilities and real-time assessment data exchanged between control centers. However, operational communications to generation plants, substations, and distributed resources fall outside this regulatory scope, even when carrying similar grid control data. State Public Utility Commissions and Public Service Boards oversee distribution utilities with requirements that vary significantly across jurisdictions. The Federal Communications Commission regulates telecommunications carriers but lacks authority over the operational traffic these networks carry for utilities. This fragmentation creates a structural problem: no single agency holds clear authority for end-to-end communications security, making it very difficult to establish consistent protections across the entire grid communications pathway.

3.2. Why Grid Transformation Accelerates Risk

Three concurrent transformations are dramatically expanding the attack surface. First, thousands of new distributed load, generation, and monitoring systems connect to the grid monthly, with California alone hosting over 1.5 million distributed solar systems, each a potential entry point. These resources have already demonstrated grid impacts through multiple events where thousands of inverters simultaneously disconnected, causing frequency disturbances across entire regions.[23] While these were not effects from cyberattacks, they illustrate the grid impact potential if adversaries could remotely trigger similar mass disconnections through compromised communications channels—a risk amplified by security researchers' discovery of thousands of internet-exposed APIs for solar inverters and battery systems that lack adequate authentication.[24]

Second, modern grid operations increasingly depend on digital communications that are essential to the operation of Advanced Distribution Management Systems (ADMS), Distributed Energy Resource Management Systems (DERMS), and other control and sensor systems. A successful communications attack could blind operators, disable automated responses, and trigger cascading failures across interconnected regions.

Finally, the proliferation of digital grid technologies creates expanded targets for increasingly sophisticated adversaries. As discussed above, nation-state actors are intensifying their focus on critical infrastructure, through persistent telecommunications intrusions, supply chain compromises of networking equipment manufacturers, and exploitation of the "black box risk" created by third-party telecommunications dependencies.

These adversaries specifically target the expanding attack surface created by cloud-connected systems and proliferating communications links. They exploit the very modernization that utilities undertake to improve grid operations. These sophisticated adversaries seek not just intelligence but pre-positioned access for future disruptive attacks. The combination of rapid technological deployment, opaque supply

chains, and pre-positioned adversaries creates a perfect storm where expanding vulnerabilities meet increasingly capable threats.

4. Recommendations

While federal regulations like NERC CIP provide strong protections within facility perimeters, critical communications beyond those boundaries remain largely unregulated. Utilities are uniquely positioned to close this gap by adopting technical measures that harden communications infrastructure against exploitation. These actions do not require waiting for policy changes—they can be implemented today to reduce risk from adversaries targeting unprotected circuits, legacy protocols, and vulnerable networking equipment. The following recommendations outline practical steps utilities can take to secure grid-supporting communications and mitigate systemic vulnerabilities.

1. **Enforce Strong Boundary Control to Keep Networking Devices Off the Internet**: Many recent compromises occurred because vulnerable networking devices were exposed to the public internet, making them easy targets for automated scanning and exploitation. Removing unnecessary internet connectivity and implementing strict segmentation reduces the attack surface and prevents adversaries from exploiting weak protocols or default credentials. This measure is particularly important for SCADA systems and field devices that were never designed for use on open networks. The principal challenge is balancing remote access needs for maintenance with security. Utilities may need to adopt secure remote access solutions rather than direct exposure.
2. **Ensure All Devices are Part of Patch Management Plans**: Unpatched networking equipment is one of the most common entry points for attackers, as demonstrated by incidents involving exposed firewalls and routers. Regular patching helps ensure that known vulnerabilities cannot be exploited to gain access to sensitive operational networks. The challenge in maintaining updated equipment lies in operational constraints. Patching may require downtime or vendor coordination, which utilities must plan for to avoid service disruptions.
3. **Use Secure Protocols Where Available**: Several legacy protocols transmit data in clear text, with limited session management or data integrity, creating opportunities for spoofing and command injection once an adversary gains network access. Where possible, utilities should enable encryption and authentication features or migrate to secure variants of these protocols. Challenges include compatibility with legacy devices and vendor support, which may require phased upgrades, protocol gateways, or interim compensating controls while longer-term modernization efforts proceed.
4. **Implement Strong Procurement Language:** Utilities can mitigate supply chain risks by embedding cybersecurity requirements into procurement contracts, such as requiring a software bill of materials (SBOMs), secure update processes, and vendor disclosure of vulnerabilities.[25] This approach addresses systemic risks beyond the ESP by ensuring new equipment meets minimum security standards before deployment. Implementation challenges include aligning procurement teams with technical security requirements and enforcing compliance across diverse vendors.
5. **Enforce Strong Access Control**: Persistent remote access and weak authentication remain major vulnerabilities, especially when vendors require continuous connectivity for support. Utilities should enforce strict access control measures, including multi-factor authentication (MFA), role-based access control (RBAC), and time-bound access for third parties. These controls reduce the likelihood of adversaries exploiting legitimate remote connections, a risk highlighted by recent incidents involving vendor firmware updates. Challenges include negotiating contractual terms with vendors and integrating access control solutions across legacy systems.
6. **Strengthen Logging and Monitoring for Communications Assets:** Effective logging and monitoring are essential for detecting misuse of remote access, attempted exploitation of networking equipment, and anomalous activity on communications that support grid operations. Utilities should ensure that communications devices and remote access gateways generate sufficient audit logs; that

those logs are retained, correlated, and regularly reviewed; and that alerts are integrated into existing security operations and incident response processes. Security information and event management (SIEM) platforms can support this function by aggregating and analyzing logs from diverse communications assets; freely available solutions, such as the Malcolm SIEM, may help lower barriers to implementation, particularly for smaller entities.[26] Where feasible, entities should define communications-focused detection use cases (for example, repeated failed connections to field devices or the appearance of unexpected remote endpoints) and ensure that incident response procedures explicitly address coordination with third-party telecommunications providers and vendors. Challenges include limited logging capabilities on legacy devices, integration with existing monitoring tools, and the need for additional analytical capacity.

The technical measures outlined in this section provide actionable steps utilities can take today to reduce risk, even in the absence of mandatory requirements. However, voluntary adoption alone may not achieve consistent protection across the industry. Long-term resilience will likely require complementary policy frameworks that establish enforceable standards and incentivize secure practices, ensuring that technical solutions become baseline expectations rather than best-effort initiatives. By combining proactive utility action with supportive regulatory evolution, the sector can close critical gaps and strengthen the security of the nation's energy infrastructure.

5. References

[1] Electricity Advisory Committee. 2025. *Resilient Communication for Grid Security: Enabling Private Broadband Networks for Critical Infrastructure*. Washington, DC: U.S. Department of Energy. https://www.energy.gov/sites/default/files/2025-06/Resilient%20Communication%20Systems_20250605_Final_Amended.pdf.

[2] Mary, Prarthana, written by Antoinette Hodes. *"2025 Threat Trend Spotlight: Edge Devices."* Security Review Magazine, May 26, 2025. Accessed January 14, 2026. https://securityreviewmag.com/?p=28272.

[3] Eclypsium. *"Network Edge Vulnerabilities and Exploits Defined: 2025."* Eclypsium Blog, December 2025. Accessed January 14, 2026. https://eclypsium.com/blog/network-edge-vulnerabilities-and-exploits-defined-2025/.

[4] Walton, Robert. 2019. "First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say." *Utility Dive*, November 4, 2019. https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.

[5] Arghire, Ionut. 2023. "22 Energy Firms Hacked in Largest Coordinated Attack on Denmark's Critical Infrastructure." *SecurityWeek*, November 14, 2023. https://www.securityweek.com/22-energy-firms-hacked-in-largest-coordinated-attack-on-denmarks-critical-infrastructure/.

[6] SecurityBuzz. n.d. "How Volt Typhoon Infiltrated a Small US Power Grid." *SecurityBuzz*. https://securitybuzz.com/cybersecurity-news/how-volt-typhoon-infiltrated-a-small-us-power-grid.

[7] Kovacs, Eduard. 2025. "China's Volt Typhoon Hackers Dwelled in US Electric Grid for 300 Days." *SecurityWeek*, March 12, 2025. https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days/.

[8] The Record. 2025. "Volt Typhoon Hackers Were in Massachusetts Utility's Systems for 10 Months." *The Record by Recorded Future News*, March 2025. https://therecord.media/volt-typhoon-hackers-utility-months.

[9] Cybersecurity and Infrastructure Security Agency (CISA). 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (Cybersecurity Advisory AA24-038A).* U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[10] Ibid.

[11] Viasat. n.d. "KA-SAT Network Cyber Attack Overview." *Viasat*. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.

[12] Reve. 2022. "Over 95 per Cent of Wind Turbines Back Online Following Disruption to Satellite Communication." *REVE – News of the Wind Sector in Spain and in the World*, April 21, 2022. https://evwind.aeeolica.org/2022/04/21/over-95-per-cent-of-wind-turbines-back-online-following-disruption-to-satellite-communication/85745.

[13] CyberNews. 2022. "Chinese Routers with Backdoors Sold in Walmart, Amazon & eBay." *CyberNews*, November 2022. https://cybernews.com/security/walmart-exclusive-routers-others-made-in-china-contain-backdoors-to-control-devices/.

[14] Intrucept Labs. 2025. "RCE Risk in D-Link Routers Due to Hardcoded Telnet Credentials (CVE-2025-46176)." *Intrucept Labs Security Advisory*, May 2025. https://intruceptlabs.com/2025/05/rce-risk-in-d-link-routers-due-to-hardcoded-telnet-credentials/.

[15] DualMedia. 2025. "Unpatched Firmware: Router and Extender Risks Linger 11 Years On." *DualMedia*, September 2025. https://www.dualmedia.com/wireless-vulnerability-unpatched/.

[16] CSO Online. 2025. "FBI Warns That End of Life Devices Are Being Actively Targeted by Threat Actors." *CSO Online*, May 2025. https://www.csoonline.com/article/3982368/fbi-warns-that-end-of-life-devices-are-being-actively-targeted-by-threat-actors.html.

[17] Sanchez, Gabriel. 2017. "Man-In-The-Middle Attack Against Modbus TCP Illustrated with Wireshark." GIAC (GCCC) Gold Certification paper, SANS Institute, October 2017. https://sansorg.egnyte.com/dl/XQr8bgdt4JYH.

[18] Machaka, V., S. Figueroa-Lorenzo, S. Arrizabalaga, B. Elduayen-Echave, and J. Hernantes. 2025. "Assessing the Impact of Modbus/TCP Protocol Attacks on Critical Infrastructure: WWTP Case Study." *Computers and Electrical Engineering* 126: 110485. https://doi.org/10.1016/j.compeleceng.2025.110485.

[19] ESET Research. 2022. "Industroyer2: Industroyer Reloaded." *WeLiveSecurity*, April 12, 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

[20] Mandiant/Google Cloud. 2022. "INDUSTROYER.V2: Old Malware Learns New Tricks." *Google Cloud Blog – Threat Intelligence*. https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks.

[21] MITRE Corporation. n.d. "Industroyer (S0604)." MITRE ATT&CK®. https://attack.mitre.org/software/S0604/.

[22] Solarboi. 2024. "Sol-Ark Manufacturer Reportedly Disables All Deye Inverters in the US." *Solarboi Blog*, November 17, 2024. https://solarboi.com/2024/11/17/sol-ark-oem-disables-all-deye-inverters-in-the-us/.

[23] North American Electric Reliability Corporation (NERC). 2021. *NERC Report on California Solar PV Disturbances: March, August, and September 2021 Events.* Atlanta, GA: NERC. https://www.nerc.com/pa/rrm/ea/Pages/March-August-September-2021-Solar-PV-Disturbances.aspx.

[24] Forescout Research (Vedere Labs). 2025. *SUN:DOWN – Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems.* Forescout Vedere Labs. https://www.forescout.com/resources/sun-down-destabilizing-the-grid-via-orchestrated-exploitation-of-solar-power-systems.

[25] Stewart, Emma Mary, Remy Vanece Stolworthy, Shari Gribbin, Tracy Lee Briggs, and Megan Jordan Culler. 2024. *Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance.* INL/RPT-24-80434-Revision-0. Idaho Falls, ID: Idaho National Laboratory. https://www.osti.gov/servlets/purl/2473239/.

[26] Battelle Energy Alliance, LLC. 2025. "Malcolm." *Malcolm: Network Traffic Analysis Tool Suite*. https://malcolm.fyi/.