SURFING THE WAVE

Resilience Strategies for the Decentralizing Grid

National Security Perspective

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

SURFING THE WAVE

Resilience Strategies for the Decentralizing Grid

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This National Security Perspective reflects the opinion(s) of the author(s) at time of writing. It does not necessarily represent the opinion(s) of Johns Hopkins Applied Physics Laboratory sponsors.

The views expressed in this article are those of the author and do not reflect the official policy of the Department of Defense or the US government.

Appendixes are included in only the online version of the report, available at https://www.jhuapl.edu/sites/default/files/2025-3/SurfingTheWave-WEB.pdf.

COMM-24-02891

Contents

Summary v

A Grid Transformed 1
- Dispersed Generation 2
- Energy Storage 4
- Decentralized Control 5
- Risk-Based Cybersecurity Requirements for the Decentralizing Grid 7
- Charting the Way Forward 9
- Plan of the Study 13

Changing the Game: Maximizing the Security Benefits of Decentralization 14
- PRC Objectives 15
- Power Islands to Support Force Projection and Protect Society 15
- Decentralized Power Restoration 18
- Multi-Hazard Resilience 19
- Shaping the Enemy's Calculus of Benefits and Costs 21

Securing the Grid against Supply Chain Exploitation 22
- China as the Pacing Threat to Grid Supply Chains 23
- Countering the Threat 24
- Voluntary Guidelines and (As Needed) Prohibition Orders 28

Making Grid Systems Secure by Design 29
- From Spinning Mass to Digital Control 30
- Enemy Exploitation 31
- Making DERs and IBRs Secure by Design—and in Depth 33

Countering Demand-Side Attacks 37
- Electric Vehicles and Charging Stations 37
- Exploiting Advanced Metering Infrastructure 39
- The Internet of Things 40

Conclusion and Summary of Appendixes 42
- Summary of Appendixes 43

Bibliography 47

Acknowledgments 87

About the Author 87

Appendix A Resource Adequacy, Cyber Contingency Response, and Power Restoration in an Inverter-Heavy Grid 89

Appendix B Employing (and Securing) Artificial Intelligence for Grid Resilience 129

Appendix C Forging Unity of Effort across the US Electric System 139

Summary

While the ongoing transformation of US power generation, storage, and control systems provides enormous benefits, it also creates dire cyber vulnerabilities. The way to fix these vulnerabilities is not to turn back the tide of the grid's transformation, but instead to surf the wave and employ novel technology-enabled strategies for grid resilience.

Nationwide deployments of solar panels and other distributed energy resources (DERs) are rapidly decentralizing US power generation. Surging battery capabilities help grid operators manage the intermittence of such generation and respond to electric system instabilities. In addition, with increasing help from artificial intelligence (AI), energy aggregators and other non-utility startups are now gathering and controlling the flow of power from DERs.

The dispersal of generation, batteries, and control systems can enable the United States to shift to a more resilient grid architecture. By exponentially growing the number of targets that adversaries must disrupt to black out the electric system, we can greatly complicate their attack planning and execution. Over time, we may also be able to exploit the "grid-forming" capabilities of advanced batteries and their power electronics to help restart the grid if outages occur and accelerate the restoration of power to hospitals, military bases, and other priority loads.

Yet, decentralization is not a panacea. Accelerated construction of large gas-fired generators, nuclear power plants, and hydro installations is essential to meet soaring US demand for power and compensate for variable solar and wind power production. Gas generators are also vital to quickly respond to grid disturbances created by severe weather—or, potentially, by cyberattacks.

Furthermore, DERs can only bolster grid resilience if they themselves can survive attack. The Department of Energy (DOE) warns that "malicious actors are positioned well to enter DER energy systems."[1] If adversaries can exploit vulnerabilities that are widely shared by these systems, they could simultaneously halt DER power production across multiple US regions. As utilities increasingly tie DERs to the high-voltage transmission infrastructure that provides the grid's backbone, DER expansion poses growing risks to the US electric system as a whole.

Cybersecurity standards for DERs lag far behind these risks. Some state public utility commissions regulate DERs and have established valuable guidelines to protect them. But compliance with such guidelines is voluntary; most states lack mandatory, enforceable cyber requirements, especially for the energy aggregators who integrate DERs and typically have little or no cyber expertise. The grid's transformation is accelerating precisely where its security is weakest.

The way to remedy these dangers is not to ban advanced grid technologies. It would be wholly impractical to reverse the spread of DERs, batteries, and localized control systems. Rather, DOE, industry, and regulators should develop and implement a cyber resilience strategy to capitalize on these advances and strengthen US security in ways that were never before possible.

That strategy should focus on attack vectors that pose especially severe risks of creating simultaneous, wide-area blackouts. The strategy must also account for a widening gap: deployments of advanced digital

[1] DOE, *Cybersecurity Considerations*, 16. See also FBI, *Expansion of US Renewable Energy Industry*.

grid devices and AI-enabled control systems are outstripping the creation and enforcement of requirements to secure them, especially for DERs. Closing that gap will require a multiyear campaign to remedy existing vulnerabilities and build security into the evolving grid. The United States can also shape the grid's evolution to help prevent enemy leaders from achieving the goals they would seek in striking the electric system, and thereby help deter attacks.

Principal findings and recommendations from this study include the following:

- *Reduce vulnerabilities to supply chain compromises.* The US electric system is riddled with software and hardware produced wholly or in part by the People's Republic of China (PRC). The United States should prohibit the purchase of products identified by DOE as posing catastrophic risks to the grid. DOE's national laboratories and their industry partners must also ramp up testing of such products to identify compromises, and share their findings with utilities and other customers much more extensively than is done today. However, because the US grid is so dependent on Chinese products, DOE should phase in prohibition orders (and bolster incentives to produce domestic alternatives) to ensure that utilities can preserve the grid's reliability.
- *Build in security in depth to mitigate "Living off the Land" (LotL) attacks.* The PRC is pre-positioning malware on the US electric system to enable it to access and misoperate grid devices and controls. US and allied product manufacturers must help grid operators strengthen layered defenses by (1) building improved security into DER communication networks and protocols; (2) limiting adversaries' ability to manipulate devices they access to create blackouts; and (3) enabling DER management systems to reduce the impact of such LotL attacks at scale. Regulators should also require DER system operators to deploy only products that meet industry and government security guidelines.
- *Strengthen resilience against load manipulation.* With the rise of electric vehicles, the Internet of Things, and other controllable loads, adversaries have growing opportunities to rapidly spike and slash the demand for power and (paired with attacks on power supplies) create system-wide instabilities. Piecemeal efforts are underway to secure loads against manipulation. DOE should use the new energy sector industrial base to integrate and accelerate such measures that benefit grid resilience.
- *Bolster deterrence by denial and resilience.* Deterrence has traditionally focused on convincing enemy leaders that if they attacked, the United States would respond by inflicting costs they would deem unacceptable. Advanced technologies can further strengthen deterrence by helping deny the benefits adversary leaders expect to achieve by striking the grid. The US Intelligence Community has identified the specific political and military goals the PRC would seek in attacking US infrastructure. DOE should incentivize deployment of AI-enabled microgrids and advanced power restoration capabilities, as well as other ways of leveraging DERs to protect critical US civilian and military functions, and help tilt Xi Jinping's calculus of the benefits and costs of grid attacks in our favor.

Appendixes[2] provide supporting details for these recommendations and examine related opportunities to strengthen the reliability and cyber resilience of the emerging grid, including measures to expand all types of generation to serve booming AI data center loads and initiatives to secure the AI tools that are crucial to support DER operators' and grid defenders' decision-making.

[2] Appendixes are included in only the online version of the report, available at https://www.jhuapl.edu/sites/default/files/2025-3/SurfingTheWave-WEB.pdf.

A Grid Transformed

Hardly any owners of distributed energy resources (DERs) or larger-scale solar, wind, and battery assets connected to high voltage transmission systems installed them to strengthen national security. Decarbonization goals, congressional spending, and restructured energy markets have driven those projects. With President Trump's declaration of a national energy emergency, federal grid-related policies are drastically changing.[1]

Yet, while security goals did little to spur the deployment of solar, wind, and battery energy storage systems, the United States now has an opportunity to leverage the nationwide dispersal of these resources (together with greatly increased nuclear and gas-fired generation) to bolster the grid's resilience against People's Republic of China (PRC) attacks.

Predicting how the electric system will evolve is fraught with uncertainties. The latest surprise: the soaring, unanticipated demand for power from data centers (especially those that provide artificial intelligence, or AI, services) and other new loads.[2] Additional energy policy initiatives launched by the Trump administration or the emergence of technological wild cards, such as the rise of fusion-based generation, could further upend projections of the grid's future.

Nevertheless, tectonic shifts are underway in the US electric system. Three trends are altering the grid's architecture:

(1) Widely dispersed deployments of solar and wind generation assets, especially DERs that are tied to local distribution systems and employ advanced power electronics to support the grid's reliability. On the horizon: small modular reactors (SMRs) and enhanced geothermal systems that would further distribute US generation

(2) The nationwide growth of battery energy storage systems (BESS) that help grid operators manage the variability of solar and wind power output and keep the grid reliable

(3) The spread of distributed energy resource management systems (DERMS) and other localized capabilities to control power flows, including from DERs to the high-voltage transmission infrastructure of the bulk power system (BPS)[3]

These changes are decentralizing the grid.[4] They also increase the danger that coordinated, multiregional cyberattacks against DERs and their control systems will disrupt the BPS. Yet, despite the growing importance of DERs to grid reliability and national security, the United States primarily relies on voluntary cybersecurity guidelines for distribution systems. Voluntary measures were adequate when cyberattacks on those systems could inflict only localized, limited blackouts. Those days are gone.

Moreover, while US cyber strategies call for building security into the evolving grid, we are deploying advanced digital devices and grid control software faster than we are implementing measures to secure them. We need a new approach to counter the systemic risks created by DERs and—at the same time—shape grid decentralization to exploit novel, game-changing opportunities to counter enemy attack objectives.

[1] Exec. Order 14156; Exec. Order 14154; White House, *Temporary Withdrawal*; and DOE, *American Energy Dominance*.

[2] Chandramowli et al., *Power Surge*; and Olivio, "Drive to Old Power Source: Coal."

[3] The BPS comprises "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy" (NERC, *Glossary*, 8).

[4] For an overview of grid decentralization, see NERC, *Cyber Security for Distributed Energy Resources*, 1–2.

Dispersed Generation

While over five million solar-powered systems are now deployed across the United States, a much smaller number of multi-megawatt natural gas, nuclear, coal, and hydroelectric power plants remain essential to meet US electricity needs.[5] Natural-gas-fueled generation remains the largest source of power for the US grid, providing 43 percent of US electricity.[6] Nuclear (19 percent), coal (16 percent), and hydroelectric generation (6 percent) are significant contributors as well.[7] Appendix A[8] examines the imperative to expand these centralized resources to meet future requirements for electricity, together with DERs, SMRs, and other more recent types of generation, which together can help achieve Secretary of Energy Chris Wright's goal of providing abundant American energy.[9]

These large-scale plants have provided for the traditional one-way flow of power from BPS generation and high-voltage transmission systems to local distribution utilities, which in turn provide electricity to their final customers. Natural gas and hydro resources also provide many of the "essential reliability services" grid managers need to balance generation with load and prevent the spread of instabilities.[10]

The expansion of solar and wind installations is altering this mix of generation resources, creating novel two-way power flows between distribution systems and the BPS and posing unprecedented challenges to grid reliability. As of 2024, solar produced only 5 percent of US power.[11] But a February 2025 assessment by the US Energy Information Administration (EIA) projects that solar's share of US generation will grow to 8 percent in 2026, spurred by an expected 45 percent increase in solar generating capacity between 2024 and 2026.[12] And while long-term projections are vulnerable to policy changes and other variables, the EIA estimates that the share of total US generation from renewables (mainly solar and wind power) will grow to 44 percent in 2050.[13]

Not only is solar and wind power growth altering the US resource mix, but it is also creating far more numerous and geographically dispersed points of power production.

The North American Electric Reliability Corporation (NERC), which develops and enforces reliability and cyber protection standards for the BPS, offers a still more striking assessment. Inverter-based resources (IBRs) constitute 85 percent of new generation under development for

[5] SEIA, "America Exceeds Five Million Solar Installations."

[6] EIA, "Short-Term Energy Outlook," "Electricity Generation by Energy Source," and "Electricity Explained."

[7] EIA, "Electricity Generation by Energy Source." All figures are as of 2023, the latest annualized data that the EIA has made available at the time of writing.

[8] Appendixes are included in only the online version of the report, available at https://www.jhuapl.edu/sites/default/files/2025-3/SurfingTheWave-WEB.pdf.

[9] DOE, *American Energy Dominance*, action 1.

[10] Essential reliability services (ERS) constitute support for frequency, ramping, and voltage control (NERC, *Essential Reliability Services*, 2). As NERC emphasized in December 2024, "natural gas-fired generators are a vital BPS resource. They provide ERS [essential reliability services] by ramping up and down to balance a more variable resource mix and are a dispatchable electricity supply for winter and times when wind and solar resources are less capable of serving demand" (NERC, *2024 Long-Term Reliability Assessment*, 8). Pages 35–36 of NERC's assessment examine the problems of ensuring the availability of ERS in an inverter-based resource (IBR)/DER heavy grid.

[11] EIA, "Electricity Generation by Energy Source."

[12] EIA, "Short-Term Energy Outlook."

[13] Linga, "Renewable Generation." Under this projection, the contribution of hydropower remains largely unchanged through 2050, and other renewable sources of power generation, such as geothermal and biomass, collectively remain less than 3 percent of total generation. See also LBNL, "Grid Connection Requests Grow."

connecting to the BPS.[14] NERC chief executive officer Jim Robb states that solar and wind projects seeking such connections are now "twice the size" of the existing one-terawatt generation capacity of the United States.[15]

As noted above, steps by the Trump administration and Congress to reverse grid decarbonization policies, eliminate tax credits and project funding for solar and wind installations, and limit federal leases for offshore wind projects will almost certainly cut the rate of growth of IBRs/DERs.[16] Supply chain problems, permitting delays, and constraints on transmission capacity for interconnections are also slowing the pace of solar and wind deployments.[17]

Yet, projects already being completed will lock in a massive increase in the scale and nationwide distribution of solar generation. The EIA estimates that developers and power plant owners added 62 gigawatts of new utility-scale solar-electric-generating capacity in 2024 (with utility-scale defined by the EIA as one megawatt or more).[18] Construction of residential solar systems and other smaller distribution-level deployments accelerated in 2024 as well, helping boost the Department of Energy (DOE) projected total of 2025 DER capacity to approximately 380 gigawatts. Wind turbines (which are typically tied to the BPS rather than distribution systems) are being increasingly deployed as well, accounting for 13 percent (or 8.2 gigawatts) of the new US generation capacity that was anticipated to come online by the end of 2024.[19]

Not only is solar and wind power growth altering the US resource mix, but it is also creating far more numerous and geographically dispersed points of power production. In addition to the five million residential and other distribution-level solar installations now deployed nationwide, the United States has 74,833 wind turbines deployed in forty-five states and nearly ten thousand utility-scale solar-generating facilities in operation or under development.[20] The potential deployment of SMRs and microreactors could further the decentralization of US power generation, as could the construction of advanced geothermal systems, hydrogen fuel cells, and other new types of resources suitable for dispersed siting.[21]

The rise of advanced power electronics underlies the emergence of all of these decentralized power sources. In particular, solar, wind, and battery energy storage systems are IBRs: they rely on inverters and other power electronics to deliver the electricity they generate to the grid.[22] NERC emphasizes that "inverter-based resources are now found everywhere across the bulk power system (BPS) in North America and are the most significant driver of grid transformation today."[23] Solar,

[14] NERC, *2024 Long-Term Reliability Assessment*, 144.

[15] Walton, "NERC Wary of 100 GW." For similar projections of solar and wind growth relative to existing US generation capacity, see LBNL, "Grid Connection Requests Grow"; and DOE, *Solar Futures Study.*

[16] White House, *Temporary Withdrawal.*

[17] Walton, "'Explosive' Demand"; and NERC, *2024 Long-Term Reliability Assessment*, 6.

[18] Suparna and Tsai, "Solar and Battery Storage." On the definition of utility-scale generation, see EIA, "Electricity Explained." Note that wind capacity additions have slowed in the last two years owing to supply chain, regulatory, and cost impediments to their deployment.

[19] DOE, "DOE Cybersecurity Report."

[20] Hoen et al., United States Wind Turbine Database; SEIA, "America Exceeds Five Million Solar Installations"; and SEIA, "Utility-Scale Solar."

[21] Liou, "Small Modular Reactors"; and Blankenship et al., *Next-Generation Geothermal Power*.

[22] As defined by the Federal Energy Regulatory Commission (FERC), "IBRs are solar photovoltaic, wind, fuel cell and battery storage resources that use power electronic devices to change direct current power, produced by generators, to alternating current power, to be transmitted on the bulk-power system" (FERC, "FERC Proposes IBR Standards").

[23] NERC, *Introduction to Inverter-Based Resources*, 1. NERC "is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces reliability standards; annually assesses seasonal and

wind, and battery DERs also rely on inverters but are smaller in scale and are connected to distribution systems versus the BPS.[24]

Many currently deployed inverters stop providing power when grid disturbances occur, magnifying those disturbances and creating broader risks to grid reliability. Inverter manufacturers now sell versions that can "ride through" such events and help grid operators limit their impact. Sophisticated new sensors and digital capabilities are helping grid protection devices, energy management systems, and other key elements of the electric system adapt to the expansion of DERs and IBRs. But these advanced capabilities also carry risks—above all, that adversaries will access and exploit them to create wide-area outages.

Energy Storage

When the sun stops shining and the wind stops blowing in a given region, power deliveries vanish from that area's solar and wind IBRs. Interregional transfers of electricity via high-voltage systems can help mitigate this intermittence. Natural gas generators can also rapidly respond to shortfalls in DER/IBR-produced power, with nuclear plants providing reliable 24/7 "baseloads" of electricity. However, BESS play an increasing role in meeting power requirements for inverter-heavy electric systems. In tandem with solar and wind generation, massive growth is underway in battery storage to help grid operators manage the variable output of these energy sources. The EIA projected that storage would nearly double in 2024, as developers added a planned 14.3 gigawatts of battery storage to the existing 15.5 gigawatts. Total battery storage capacity is projected to rise to 40 gigawatts in 2025.[25]

DOE is also collaborating with industry to extend the number of hours during which BESS can provide power. Currently, most systems can deliver energy for four hours if they are fully charged and discharged at their maximum power rating before needing to be recharged. DOE is partnering with industry to develop long-duration energy storage, focused on reducing storage costs by 90 percent for storage systems that deliver electricity for at least ten hours. DOE–industry initiatives are also developing and deploying advanced electrochemical, mechanical, thermal, and other energy storage systems as alternatives to lithium-based batteries.[26]

BESS are also helping drive the expansion of a novel contributor to decentralized grid operations: virtual power plants (VPPs). These virtual plants are aggregations of DERs, such as rooftop solar with behind-the-meter batteries, electric vehicles (EVs) and their charging stations, smart buildings and their controls, and other flexible loads that can balance electricity demand and supply and "provide utility-scale and utility-grade grid services like a traditional power plant."[27] DOE's goal has been to deploy 80 to 160 gigawatts of VPPs by 2030, tripling their current capacity.[28]

In addition, smaller-scale energy aggregators are pairing BESS with solar systems at an accelerating pace. Aggregators bundle power provided by multiple residential solar panels and their battery systems, as well as other DERs. They then sell that power in electricity markets managed by regional transmission organizations and independent

long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel" (NERC, "About NERC").

[24] FERC defines DERs as "small-scale power generation or storage technologies (typically from 1 kW to 10,000 kW) that can provide an alternative to or an enhancement of the traditional electric power system" and are "located on an electric utility's distribution system, a subsystem of the utility's distribution system or behind a customer meter" (FERC, "FERC Order No. 2222: Fact Sheet").

[25] Suparna and Tsai, "Solar and Battery Storage."

[26] DOE, "Long Duration Storage Shot."

[27] Downing et al., *Virtual Power Plants*, 2.

[28] Downing et al., *Virtual Power Plants*, 2.

system operators.[29] In addition, utilities are building hundreds of "hybrid" power plants that combine much larger solar and wind generation capacity with BESS. One of the largest, the Gemini hybrid plant in Nevada, has a photovoltaic capacity of 690 megawatts and battery storage of 380 megawatts.[30]

The nationwide construction of these hybrid plants, together with VPP and aggregator projects, will further the grid's decentralization and help manage the intermittence that solar and wind power entail. In the years to come, advances in battery inverters and other electronics could also enable BESS to help restore power if adversaries create wide-area blackouts.[31]

However, BESS' dependence on inverters makes them vulnerable to many of the same attack vectors as wind and solar assets. Ninety to 100 percent of BESS deployed in the United States have at least one PRC component. The largest battery provider: the Contemporary Amperex Technology Co., Limited (CATL), which has close ties to the Chinese military and whose products are banned from Department of Defense (DOD) contracts but are still being installed across the US grid.[32] And as advanced batteries offer additional benefits to the grid, the risks they pose will expand as well. DOE cautions that if batteries and other DERs gain capabilities to help restore power, attackers can seek to maliciously operate those capabilities to cause continuous restoration failures and extend outages indefinitely.[33]

Decentralized Control

That leaves the most difficult challenge: how can grid operators manage the flow of power from millions of solar, wind, and storage assets? In particular, how can they maintain the electric system's reliability, defined by NERC as ensuring "that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements"?[34]

Grid decentralization creates complex new risks to BPS reliability. In a 2023 report on those risks, NERC found that "rapid resource deployments—on both transmission and distribution systems and with both centralized and distributed resources—are resulting in BPS operating conditions that were not within the original planning criteria." Moreover, with the accelerating integration of new types of generation, storage systems, and inverters to control their power flows, "the cadence of innovation and deployment is overwhelming traditional grid operation software platforms, interconnection processes, and performance standards."[35]

AI is coming to the rescue but is also introducing new attack surfaces.

The problems of managing widely dispersed DERs are especially severe. The most detailed study yet published on grid modernization, the National Academy of Sciences' report on the future of electric power in the United States, finds that:

[29] FERC defines a DER aggregator as "an entity that aggregates one or more distributed energy resources for purposes of participation in the capacity, energy and ancillary service markets of the regional transmission operators and independent system operators" (FERC, *Final Rule: Participation of Distributed Energy Resource Aggregations*, 85).

[30] Suparna and Tsai, "Solar and Battery Storage"; and LBNL, "Hybrid Power Plants."

[31] The second section of this report examines opportunities and impediments for BESS to support restoration.

[32] DOE, *Battery Energy Storge Systems,* 35–37, 43; DOD, *Designation of Chinese Military Companies*; and Shepardson, "CATL to Restricted List."

[33] DOE, *Cybersecurity Considerations*, 28–29.

[34] Control center functions are specified in NERC, *Glossary*, 12. The definition of reliability is on p. 26 of the glossary.

[35] NERC, *2023 ERO Reliability Risk Priorities Report*, 23.

> At present, most operators of high-voltage grids are unable to assess conditions at the edge of the grid, particularly in real time, even though such conditions affect loads and system operations on the high-voltage, bulk power system. DER-induced bidirectional power flows require coordination with existing distribution-system operations and protection equipment, but also potentially with operators of bulk power systems. In this context, utilities are developing Distributed Energy Resource Management Systems (DERMS), platforms designed to offload the task of coordinating millions of DER to a third party. Even with this type of delegation, the complexity and cost associated with managing DER is immense, and extensive and coordinated planning will be necessary.[36]

The growing number and diversity of DER operators magnify these coordination problems. Until recently, grid assets were operated by traditional BPS and local distribution system utilities. With the rise of aggregators, VPPs, and other new types of power companies, a much wider array of entities now manages DER power flows—typically with operational and cybersecurity staffs that are much smaller than those of utilities.

AI is coming to the rescue but is also introducing new attack surfaces. AI-enabled DERMS and other software systems give large aggregators, VPPs, and distribution system operators (DSOs) automated and increasingly effective decision support tools to control power flows and help balance power supplies with demand—an essential reliability service (ERS).[37]

DOE's report *AI For Energy: Opportunities for a Modern Grid and Clean Energy Economy* states that AI is also an "essential tool" for facilitating coordination of bidirectional power flows between the BPS and distribution systems and can help operators detect, diagnose, and respond to grid disturbances.[38]

Yet, while AI tools are becoming essential to manage decentralized grid operations, no requirements exist to secure these tools from enemy compromise and exploitation. DOE's report on AI identifies a number of potential AI risks and calls for the development of best practices to mitigate them (DOE's Office of Cybersecurity, Energy Security, and Emergency Response has already embarked on such efforts with industry partners).[39] The National Institute of Standards and Technology (NIST) has also issued an AI risk management framework that provides voluntary recommendations to help "foster the responsible design, development, deployment, and use of AI systems over time."[40] Meanwhile, we are deploying AI-enabled DERMS and other AI systems to transform grid operation without first assessing whether such voluntary guidelines are adequate, especially against adversaries that DOE warns are already well positioned to enter DER systems.[41]

Communications pose a further quandary. Managing the massive (and extraordinarily complex) data flows required to control decentralized grid operations, especially given the variable power output of solar and wind resources, constitutes a growing challenge for distribution utilities, aggregators,

[36] NASEM, *Future of Electric Power*, 50. On additional sources of complexity and increasing requirements for automated decision-making, see NERC, *2024 State of Reliability*, 39.

[37] NREL, "Distributed Optimization and Control" and "Advanced Distribution Management Systems"; Lagos, "Winds of Change"; Pratt, "Rescuing the Grid"; and GridScape, "Symbiotic Role."

[38] Benes, Porterfield, and Yang, *AI for Energy*, 20–21. Appendix B in this report examines the uses of AI for grid operation and the risks that adversaries will exploit US dependence on those AI applications.

[39] Benes, Porterfield, and Yang, *AI for Energy*, 22–25, 40.

[40] NIST, *Artificial Intelligence Risk Management Framework*, 2.

[41] DOE, *Cybersecurity Considerations*, 16, 21–29.

and VPPs.[42] Advanced network technologies and third-party service providers have emerged to meet these requirements. Wireless, Internet Protocol (IP), and cloud-based communications networks are now critical enablers of localized DER control, with the latter used to manage many (if not all) BESS fleets.[43]

These networks offer a growing attack vector as well. The NIST report *Cybersecurity for Smart Inverters* notes that these devices often use the internet to connect with cloud-based management capabilities, which increases the exposure of inverters to cyber threats and adversary misoperation.[44] The rapid growth and digital "smartness" of internet-connected DERs contributes to these risks, with NERC predicting that such connectivity will continue to expand "exponentially."[45] NIST and the industry standards-setting organizations offer detailed guidelines to make DER communications links less vulnerable. But, NIST also found that many inverters being deployed today lack the capabilities needed to implement such guidelines.[46] Furthermore, DOE has identified multiple pathways by which adversaries can exploit DER communications vulnerabilities, including direct manipulation of wide-area power system devices.[47]

These security problems are exacerbated by sophisticated enemy capabilities to penetrate cloud defenses. NIST and other organizations have provided an array of voluntary guidelines to strengthen cloud access controls and other attack surfaces.[48] Nevertheless, as in the December 2024 PRC attack on the Department of Treasury, cloud-based service providers remain vulnerable.[49] Power companies can minimize these risks by retaining in-house computational platforms. As in the case of Southern Company, Xcel Energy, and a growing number of other major utilities, companies can also avoid the dangers of relying on vulnerable third-party telecommunications service providers (breached by the PRC in November 2024[50]) by building their own private networks for critical communications.[51] But very few distribution systems, aggregators, and VPPs will be able to afford such networks.

Risk-Based Cybersecurity Requirements for the Decentralizing Grid

The first step to manage the cyber risks created by the growth of distributed resources and the technologies supporting them is to bridge the regulatory divide between the BPS and local distribution systems. The BPS is regulated by NERC and the Federal Energy Regulatory Commission (FERC). For decades, they have partnered to establish mandatory, enforceable cybersecurity standards for the BPS. That work provides a well-established foundation for NERC's ongoing analysis of possible security requirements for utility-scale IBRs directly connected to the BPS.

Voluntary regulatory strategies were adequate when distribution-level disruptions could create only localized blackouts. Those days are gone.

Local distribution systems operate under a fundamentally different regulatory framework. State public utility commissions (PUCs) and other state

[42] NARUC, *Regulator's Financial Toolbox Brief*; DOE, *Power Grid and Communications Interdependencies*; and DOE, *Battery Energy Storge Systems.*

[43] NARUC, *Regulator's Financial Toolbox Brief*; and DOE, *Power Grid and Communications Interdependencies.*

[44] McCarthy et al., *Cybersecurity for Smart Inverters*, 1, 3, 10–11.

[45] NERC, *Cyber Security for Distributed Energy Resources.*

[46] McCarthy et al., *Cybersecurity for Smart Inverters*, 12, 37–44.

[47] DOE, *Cybersecurity Considerations*, 24.

[48] NIST, *General Access Control Guidance for Cloud Systems.*

[49] Hardikar, Letter.

[50] CISA and FBI, *Joint Statement.*

[51] Engle, "Utilities Are Ditching Carriers."

and local authorities regulate these systems.[52] Very few states have adopted mandatory, enforceable cybersecurity standards that are remotely equivalent to those that exist for the BPS. Instead, state regulators are following two basic approaches to manage emerging distribution-level risks.

First, PUCs are beginning to implement the recommendations of the cybersecurity baselines issued by the National Association of Regulatory Utility Commissioners (NARUC). The baselines offer guidelines to help PUCs, distribution utilities, and DER operators and aggregators secure their systems. However, while these recommendations are sound, their adoption remains purely voluntary.[53]

Second, state PUCs can adopt guidelines developed by industry. Standards created by the Institute of Electrical and Electronics Engineers (IEEE) exemplify these opportunities. IEEE Standard 1547-2018 establishes DER performance requirements that PUCs should adopt and enforce as a condition for connecting those resources to local electric systems.[54] IEEE Standard 1547.3-2023, adopted in December 2023, provides DER cybersecurity guidelines.[55] IEEE Standard P2030.14 offers a guide for VPP functions and control systems, with UL and other industry entities setting standards for DER-related equipment.[56] Like NARUC's baselines, these guidelines are valuable, but nothing requires PUCs to adopt them. As of May 2024, only a dozen states had fully implemented IEEE's DER performance standards. Adoption of IEEE's cybersecurity recommendation for DERs lags far behind even that pace, with only California and a handful of other states exploring their enforcement.[57]

Voluntary regulatory strategies were adequate when distribution-level disruptions could create only localized blackouts. With the escalating contribution of distributed generation to the BPS and the rise of aggregators' and VPPs' automated, AI-enabled controls, attacks on distribution systems can create far broader dangers. NERC warns that the compromise of a DER aggregator's VPP system could lead to malicious software being introduced into DERs "across a large geographic footprint," resulting in "widespread outage of these assets." NERC also notes that its cybersecurity standards do not apply to DER aggregators, even though aggregators may become the equivalent of "generation control centers in the near future."[58]

Managing the risks posed by aggregators and VPPs entails additional challenges. While PUCs might use interconnection agreements with regulated distribution utilities to ensure aggregator and VPP compliance with cybersecurity guidelines, some commissioners doubt whether the state laws governing their regulatory purview provide sufficient authority to do so.[59] State legislatures should grant PUCs explicit authority to use interconnection agreements and other mechanisms to enforce aggregator/VPP compliance and oversee measures by these operators to securely install and operate PUC-approved networks and devices.

Equivalent security measures will be necessary for rural electric cooperatives and public power utilities. Forty-two million people and 56 percent of US territory is served by rural cooperatives, including

[52] Public power utilities and rural cooperatives are overseen by different authorities than the PUCs that regulate local distribution systems. Subsequent portions of this section and Appendix C examine these regulatory structures and their implications for forging consistent, nationwide cybersecurity standards for DERs.

[53] NARUC, "Cybersecurity Baselines"; and NARUC, *Scope and Prioritization of the Baselines*.

[54] IEEE, IEEE 1547-2018.

[55] IEEE, IEEE 1547.3-2023.

[56] IEEE, IEEE P2030.14; UL, *PV Inverter and BESS Converters Certification*; and UNIFI Consortium, *Specifications for Grid-Forming Inverter-Based Resources*.

[57] CPUC, *Working Group Report*.

[58] NERC, *Cyber-Informed Transmission Planning*, 6, 8.

[59] Author interview with Richard Mroz, former president of the New Jersey Board of Public Utilities, June 28, 2024.

many remote but vital military bases. Public power utilities serve an additional fifty-four million Americans. These systems and their cybersecurity efforts are overseen not by PUCs but by their individual sets of elected officials and governing boards.[60] With the expansion of DERs connected to cooperatives and public utilities, as well as local distribution systems, it is imperative to coordinate nationwide security measures across this diverse regulatory environment. Appendix C proposes steps to implement such a coordinated approach.

Moreover, neither DOE nor any other organization has a comprehensive registry that identifies VPPs and aggregators nationwide. Managing the systemic dangers posed by these power companies will be difficult if we don't even know who they are. For the BPS, NERC is identifying and registering IBR owners and operators that are not currently registered, thereby making those assets subject to NERC's mandatory reliability and cybersecurity standards.[61] DOE should collaborate with NARUC and other distribution-focused associations to develop an equivalent nationwide registry of aggregators and VPPs.

Charting the Way Forward

The most immediate way to impose mandatory cybersecurity standards for distribution-level systems would be for Congress to amend the Federal Power Act to authorize NERC and FERC to extend their regulatory authorities to those systems. But any such amendment would be dead on arrival. For decades, legislators have preserved state and local responsibilities for regulating distribution systems. Efforts to strip that authority would raise profound constitutional issues regarding the power of Congress under Article I, Section 8, to legislate on activities that do not constitute interstate commerce (i.e., local distribution systems). In addition, NERC is not proposing to extend its authorities to the distribution level.

To account for the growing risks that DERs pose to the electric system as a whole, and to move beyond the slow and uneven state adoption of voluntary guidelines, state regulators must lead the charge. They can draw on current initiatives and harsh lessons from history to do so.

NARUC's cybersecurity baselines are part of a much broader array of collaborative cybersecurity efforts between PUCs, DOE, national laboratories and universities, and industry partners. DOE's Office of Cybersecurity, Energy Security, and Emergency Response is sponsoring dozens of such projects, including the Clean Energy Cybersecurity Accelerator, the Energy Cyber Sense program, and (in 2024 alone) sixteen new cybersecurity research and development efforts across six states.[62] DOE is also helping apply secure-by-design and secure-by-default principles to inverters, BESS, and distributed control system software, thereby enabling the operation and coordination of hundreds of thousands of distributed energy assets with integrated advanced cybersecurity control technologies.[63]

Collaboration among NERC, FERC, and NARUC is also expanding, enabling PUCs to borrow from BPS-level regulatory and technical initiatives and apply them to help meet state priorities.[64] An

[60] Public power utilities are entities of local or state governments and are typically regulated by elected or appointed boards, mayors, or city council members. Rural electric cooperatives are private, not-for-profit businesses. They are owned by their consumer members, who elect governing board members and are required to return any excess revenue to their members (APPA, *Public Power*, 2; and NRECA, "What We Do").

[61] This initiative, which implements FERC's order in Docket No. RD22-4, entitled "Registration of Inverter-based Resources," is "registering owners and operators of non-BES [bulk electric system] IBRs with aggregate nameplate capacity of greater than or equal to 20 MVA, delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV" (NERC, *Frequently Asked Questions*).

[62] DOE, "Nearly $23 Million" and "$45 Million."

[63] White House, *Enhancing the Digital Ecosystem*.

[64] FERC, "Federal-State Current Issues Collaborative."

immediate and especially significant opportunity for such cooperation lies in securing the advanced performance capabilities of DERs/IBRs. In October 2023, FERC issued Order No. 901, which requires NERC "to develop new or modified reliability standards that address reliability gaps related to inverter-based resources."[65] NERC subsequently proposed those standards to require that IBRs be able to ride through frequency and voltage disturbances and continue to deliver power when such events occur.[66] Ensuring that DERs have equivalent reliability features constitutes an intense and valuable area of BPS-distribution level collaboration.[67]

Order 901 did not require NERC to develop IBR-specific security standards. However, the commission did direct NERC to "evaluate whether there are gaps that must be addressed."[68] As that analysis goes forward, NERC, NARUC, and their partners should collaborate to create standards that help secure both DERs and IBRs.

The trick: establish and enforce security requirements *before* adversaries strike.

Yet, NERC's adoption of mandatory security requirements also offers a cautionary tale. For years, the electric industry and its allies in Congress resisted suggestions that voluntary reliability guidelines were no longer adequate for a tightly interconnected grid. The move toward mandatory, enforceable reliability standards only occurred after the catastrophic blackout of August 14, 2003. That event highlighted the risks of cascading, multistate disruptions and other systemic dangers that had been intensifying for years and created the political will to shift from voluntary to mandatory BPS standards.[69]

A coordinated, nationwide cyberattack on DERs that causes system-wide disruptions would create equivalent pressure to establish distribution-level mandates. The trick is to establish and enforce security requirements *before* China or other adversaries strike, thereby reducing the disruption attackers will inflict on the economy, public health and safety, and the ability of US military bases to conduct response operations.

Facilitating the Transition to More Effective Regulations

Reliance on voluntary guidelines for distribution systems is so deeply rooted that only narrowly targeted, risk-based initiatives to establish mandatory standards are likely to succeed. The Cybersecurity and Infrastructure Security Agency (CISA) suggests basing risk assessments on the potential direct and indirect consequences of an incident, known vulnerabilities to various potential threats or hazards, and general or specific threat/hazard information.[70] DOE and its partners in the US Intelligence Community are well positioned to assess threats and vulnerabilities, as exemplified by the report *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*.[71]

In addition, DOE's national laboratories have sophisticated modeling capabilities to help assess the likely scope and duration of adversary-induced outages, both for DER-focused attacks and for simultaneous strikes against the BPS and distribution systems that maximize disruption of two-way power flows and exacerbate grid-wide instabilities.

[65] FERC, *Final Rule: Reliability Standards*, i.

[66] NERC, *Proposed Reliability Standards PRC-029-1 and PRC-024-4*. On December 28, 2024, FERC issued a notice of proposed rulemaking to adopt those standards with additional requirements (FERC, *Frequency and Voltage Protection Settings and Ride-Through for Inverter-Based Resources*).

[67] NERC, *Distributed Energy Resources*, 27 (voltage and frequency standards for DERs are examined in detail on pp. 38–39).

[68] FERC, *Final Rule: Reliability Standards*, 63.

[69] Nevius, *History*; and NERC, *Blackout*.

[70] CISA, *Risk Assessment Methodologies*.

[71] DOE, *Cybersecurity Considerations*

Going forward, these laboratories should intensify their analysis of how increasing DER/IBR deployments and adversary manipulation of large-scale loads could further magnify the consequences of strikes on the grid, and also help regulators assess the direct and indirect costs the United States can avoid by mandating specific security measures.

Industry input will also be crucial to assess emerging risks. Asset owners and operators, reliability coordinators, and balancing authorities have the most detailed, comprehensive understanding of their systems and of strengths and potential gaps in their cyber defenses. They can also assess the practicality of possible security requirements. From a grid defense perspective, for example, it might be desirable to ban the deployment of all Chinese-produced inverters, DERMS software, and BESS. But as will be discussed in the third section, many utilities would find it impossible—at least for the near term—to sustain reliable service without buying Chinese products. Owners/operators and vendors must help regulators target and phase the implementation of future mandates.

Of course, leadership by state and local regulators will be essential to establish cybersecurity requirements for DERs, DERMS, and other adversary targets. One of their core responsibilities will be to assess the "prudence" of proposed standards. NARUC and its partners have developed energy resilience frameworks that help regulators apply risk-based threat assessments and cost–benefit analyses to evaluate proposed investments, based in part on "costs avoided"—that is, the direct economic consequences of blackouts that would occur if a project did not go forward.[72] By incorporating consequence modeling from national laboratories and vendor assessments of the price of additional protection measures, state and local regulators will be able to focus initial mandates on those that offer the greatest security value.

Cooperation across states and US territories will also be necessary to harmonize such mandates. A patchwork of fifty-four different sets of cybersecurity requirements could give attackers valuable gaps and seams to exploit, and could create a nightmare for vendors seeking to comply with new standards. NARUC is ideally positioned to build consensus on PUC standards, in close collaboration with the National Rural Electric Cooperative Association, the Edison Electric Institute, and the American Public Power Association to include their respective distribution systems nationwide.[73]

Prioritizing Regulatory Initiatives

The risk management framework for DERs must fundamentally differ from that which has traditionally guided BPS cybersecurity. Under NERC Standard CIP-002-5.1a, *BES Cyber System Categorization*, control centers, generation plants, transmission facilities, and other BES components are ranked as high-, medium-, or low-impact cyber systems, depending on the impact the loss, compromise, or misuse of those systems could have on the reliable operation of the grid.[74] NERC's cyber protection standards scale with these categories. The most stringent requirements apply to the small number of high-impact systems; the more numerous (but less critical) medium- and low-impact systems are required to comply with less stringent standards.

That framework is no longer sufficient. In the past, it was reasonable to assume that attacks would focus on high-impact systems. However, drawing lessons learned from SolarWinds and other attacks that have compromised large numbers of

[72] McCurry and Nethercutt, "Shared Framework," 5–16. Appendix C offers additional analysis of cost avoidance and other project metrics. That appendix also examines the degree to which the federal government, versus ratepayers, should fund resilience projects that directly benefit national security versus broader service improvements for utility customers.

[73] On the imperative to establish consistent, nationwide standards, see NARUC, *Scope and Prioritization of the Baselines*, 4.

[74] NERC, *CIP-002-5.1a*.

systems, NERC warns that adversaries can use network connectivity, remote access, and other means to conduct coordinated strikes against multiple low-impact systems. The result: attacks at sufficient scale, even against systems that are of little individual consequence, can create high-impact disruptions.[75]

AI intensifies the danger of coordinated attacks by helping adversaries map and simultaneously execute attacks against vast numbers of grid assets. Moreover, with the deployment of millions of DERs, the expansion of aggregator and VPP-led control operations, and the growing importance of these dispersed systems to the grid's reliability, structural changes are heightening the potential impact of coordinated attacks. We need a risk management framework to guide the development of cybersecurity mandates for the decentralized electric system.

NERC-led efforts to bolster security requirements for high- and medium-impact systems remain vital as threats intensify. Indeed, with increasing US dependence on solar power, it is as important as ever to ensure that BPS transmission and control systems can move this variable power to where customers need it. In addition, NERC should partner with state and local regulators, grid operators, and their suppliers to reduce the dangers posed by common-mode failures—that is, adversary exploitation of vulnerabilities shared by widely deployed hardware, firmware, software, or communications networks and support services (such as cloud data storage) to cause the widespread, simultaneous disruption or misoperation of such assets.[76]

This study focuses on countering two pervasive risks of common-mode failures: (1) the corruption and exploitation of supply chains for products critical to the grid's transformation; and (2) the use of "Living off the Land" (LotL) malware and other attack vectors to misoperate advanced inverter capabilities, including those necessary to maintain the reliability of an inverter-heavy grid.

The study also proposes options to meet a more complex regulatory challenge. Efforts to counter supply chain and system misoperation threats offer the advantage of falling squarely within the authority of FERC, NERC, and their state and local counterparts. In tandem with attacks to disrupt power availability, adversaries can seek to rapidly alter the demand for electricity from EV charging stations and other controllable loads, thereby magnifying the grid instabilities their attacks create. Mitigating the load manipulation dangers entailed by EV chargers, smart buildings, and the Internet of Things (IoT) will involve multiple federal agencies and industries that have never been included in grid security mandates—and may not want to be.

The way to make this fight less one-sided is to require electric companies to exclusively deploy software, hardware, and other systems that are secure by design.

Creating a Fairer Fight

The BPS regulatory system depends on a feature that is absent in the DER ecosystem. NERC's critical infrastructure protection (CIP) standards set detailed requirements for cybersecurity but do not dictate how companies should meet them. Transmission system operators, reliability coordinators, and other BPS entities have large, well-trained

[75] NERC, *Low Impact Criteria Review Report*. For a prescient analysis of these risks and a call for NERC to "recognize the potential for simultaneous loss of assets and common modal failure in scale in identifying what needs to be protected," see NERC, Letter from Michael Assante.

[76] The nuclear power industry uses an equivalent term, *common cause failure*, to describe a similar phenomenon: the "loss of function to multiple structures, systems, or components due to a shared root cause" (NRC, "Common Cause Failure Definitions").

teams to implement protection requirements in ways that reflect their specific infrastructure characteristics and security priorities. These teams must also comply with NERC's extensive training, simulation, and exercise mandates to help them respond to attacks and restore power.

Few if any aggregators or VPPs have cyber teams with equivalent capabilities and training. Strategies to regulate these and other DER operators must account for their shortfalls in cyber expertise. Differences in cyber capabilities are still more striking between DER companies and the adversaries targeting them for attack. The PRC exemplifies this disparity. Christopher Wray, former director of the Federal Bureau of Investigation (FBI), offered an assessment of his own organization's cyber staffing versus China's. Wray testified that "if each one of the FBI's cyber agents and intel analysts focused exclusively on the China threat, Chinese hackers would still outnumber FBI Cyber personnel by at least 50 to 1."[77]

The asymmetry is still greater between the PRC and DSOs—and, indeed, vis-à-vis even the largest and most capable BPS entities. Assistance from DOE, DHS (the Department of Homeland Security), and DOD can help these potential targets of attack supplement their own resources.[78] So too can scores of cybersecurity contractors that support utilities. Even with such assistance, however, grid operators' cybersecurity teams are thoroughly overmatched by the resources of the PRC.

The way to make this fight less one-sided is not to require electric companies to match the staffs of their adversaries, but rather to require that they exclusively deploy software, hardware, and other systems that are secure by design. As defined by CISA, secure by design means that "technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure."[79] A growing number of state regulators are establishing whitelists for inverters and other products that meet state mandates to support grid reliability, and they are requiring distribution companies to buy only products that are on those lists as a precondition for interconnecting with the grid. The next step: regulators should establish equivalent requirements to deploy only those products that DOE and industry partners (including IEEE) certify as secure by design, versus cheaper products that lack such protections. The fourth section proposes options to set secure-by-design mandates for advanced inverters, together with measures by utilities to securely configure and integrate them into BPS and distribution systems.

Plan of the Study

In addition to implementing the measures proposed above to protect dispersed generation and control systems and mitigate the new attack surfaces that decentralization creates, the United States can gain still greater security benefits by developing an "upside" strategy—that is, an explicit guide to maximize the benefits of the grid's transformation. The next section provides an overview of what such a strategy should entail and ways to make it practical and affordable. The rest of the study is organized as follows.

The third section offers recommendations to protect and build diversity into grid supply chains. In particular, this section proposes how to counter China's decade-long strategy to dominate and exploit the US market for IBRs and other "clean energy" products.

[77] Quoted in Feiner, "Chinese Hackers Outnumber."

[78] DOD can also enhance utility defense by blunting cyberattacks at their sources abroad, and it can deter attacks by helping convince adversaries that they would suffer costs they would deem unacceptable if they struck. These DOD contributions to grid defense are examined in the fourth section of this report.

[79] CISA et al., *Secure by Design Software*, 8.

The fourth section proposes options to prevent the misoperation of electric system controls and digital devices through secure-by-design initiatives, using inverters as a case study but also offering preliminary recommendations for grid protection systems and other high-impact adversary targets.

The fifth section analyzes the growing dangers posed by load manipulation attacks and how DOE can structure the nascent energy sector industrial base (ESIB) to build and implement an integrated, multi-industry plan to reduce those risks.

Three appendixes supplement this analysis.[80] Appendix A offers technical details on inverter capabilities, including for maintaining reliability and restoring power in the face of ongoing cyberattacks. Appendix A also analyzes looming shortfalls in the adequacy of IBR/DERs and other resources to meet spiraling demand from AI data centers and other new types of loads.

Appendix B offers additional details on the use of AI to provide decision support for DER operators and—over the longer term—help counter AI-enabled cyberattacks in ways that humans alone cannot match. Appendix C proposes measures to help regulators and asset operators transition from voluntary to mandatory security standards and addresses the question of who should pay for what.

Changing the Game: Maximizing the Security Benefits of Decentralization

Under the grid's past architecture, we had most of our eggs (i.e., multi-megawatt generation plants, BPS control centers, and other high-impact systems) in a few baskets, against which adversaries could concentrate their cyber firepower. With millions of DERs and AI-enabled DERMS to control them, we are creating an exponentially larger number of baskets. This structural shift *could* dramatically increase the number of targets that adversaries must disrupt to create wide-area, long-duration blackouts, and thereby strengthen the grid's survivability.

Yet, additional steps will be needed to reap the potential security benefits of decentralization. While DERMS provide increasingly advanced tools to manage DER power flows and help grid operators balance generation with load, those capabilities fall short of what is needed to sustain power flows to local customers if adversaries black out the surrounding grid. Operators and their distributed resources need the ability to establish "power islands" that can segment as needed from the BPS, reliably serve the loads within their boundaries, and then reconnect with the BPS (and ideally, provide power to it) when circumstances allow.

The most familiar way to establish power islands is via microgrids, defined by DOE as "a group of interconnected loads and DERs within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid."[81] In addition, with the advances in AI controls for segmentation and power island management, and in energy storage, other options are emerging to radically increase the number and geographic scale of these islands across the United States and employ them as building blocks to create an electric system inherently resilient against cascading failures and uncontrolled separation.

Strategies to leverage grid decentralization should also seek more ambitious goals. Equipping BESS with "grid-forming" (GFM) inverters that can help restart the grid when blackouts occur is one such objective. We can also use resource dispersal to reduce the electric system's vulnerability to swarm attacks by uncrewed aerial systems (UASs), missiles, and other kinetic means, just as Ukraine is

[80] Appendixes are included in only the online version of the report, available at https://www.jhuapl.edu/sites/default/files/2025-3/SurfingTheWave-WEB.pdf.

[81] DOE, *Microgrid Overview*.

beginning to do against Russia. Finally, and most ambitious: DOE, regulators, and industry can shape all these resilience initiatives to reduce enemy leaders' confidence that they will achieve the goals they seek in striking the grid, thereby making such attacks less likely.

PRC Objectives

The 2024 *Annual Threat Assessment of the U.S. Intelligence Community* finds that Russia, Iran, and North Korea have sophisticated capabilities to attack US infrastructure.[82] However, the assessment emphasizes that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."[83] The assessment also identifies specific goals that the PRC may seek in attacking the grid and other US infrastructure:

> If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.[84]

Disrupting the electric system can help China's leaders achieve each of these objectives. In turn, denying their ability to do so should guide US efforts to shape the grid's evolution and measures to bolster its resilience. Russia and other potential adversaries may have other attack priorities. Nevertheless, consistent with the US National Defense Strategy's focus on China as the "pacing threat," this study concentrates on options to counter the PRC's objectives—or, at a minimum, intensify Xi Jinping's doubts that he can achieve them.[85]

Power Islands to Support Force Projection and Protect Society

China can seek to interfere with the deployment of US forces to the Taiwan Strait or other crisis zones by disrupting the flow of electricity inside the United States that supports such force projection. In particular, the PRC may target the electric infrastructure that enables "fort-to-port" operations, in which forces and supporting assets will move from US military bases to and through seaports on the West Coast, Hawaii, Guam, and other locations.[86]

While separation from the grid could be accomplished, it would present significant challenges.

BPS initiatives can bolster the resilience of power flows to facilities and transportation systems that enable power projection in the face of adversary attacks. For example, DOE argues that by expanding interregional transmission infrastructure, grid owners and operators could more effectively move power from areas of excess generation capacity to areas where shortfalls are occurring, improving their ability to manage the disruptive effects of severe heat waves and other extreme events.[87] Those same transmission capabilities and other BPS resilience initiatives will be valuable for supporting multiregional fort-to-port operations.

The wide dispersal of DERs and advanced technologies to manage them enables an additional line

[82] ODNI, *Annual Threat Assessment*, 22.

[83] ODNI, *Annual Threat Assessment*, 11.

[84] ODNI, *Annual Threat Assessment*, 11.

[85] On China as the pacing threat, see DOD, *2022 National Defense Strategy*, iii, 2.

[86] VanHerck and Van Ovost, "Fighting to Get to the Fight"; and RFPB Subcommittee, *Reserve Component Support*, 6–9.

[87] DOE, *Executive Summary: National Transmission Planning Study*, 1, 25.

of effort: the deployment of microgrids to serve military bases and other critical facilities. Many forts have thousands of acres on which to deploy solar and wind generation assets and distribution infrastructure. Moreover, current DOD polices support the large-scale build-out of microgrids. The US Army Climate Strategy calls for installing a microgrid on every Army installation by 2035.[88] Other US armed services and DOD components have similarly aggressive targets for microgrid construction.[89]

The port part of the equation poses greater difficulties for microgrids. The Port of Los Angeles operates thousands of electricity-dependent facilities and devices spread over 7,500 acres, including 1,932 pieces of cargo handling equipment and 22 miles of railroads.[90] Other civilian-operated ports that might be used to deploy US forces to a Far East contingency, such as the Port of Long Beach, also comprise thousands of acres and—with the electrification of port operations—will require even more dispersed resources for power distribution than today.[91]

Moreover, while military base microgrids are relatively easy to separate from the grid, civilian ports are tied to (and depend on) incredibly complex webs of distribution lines, substations, and other electric infrastructure that would need to be segmented to establish a power island. Civilian ports are typically designed for multiple points of interconnection to the grid, and many are operated as multiple radial distribution lines that are not meant to be closed except during emergencies. Hence, while separation from the grid could be accomplished, designing and constructing the "inside the port" DERs to serve cranes and other loads would be a significant challenge.[92] And where could sufficient solar wind and generation assets be sited in congested, urban-area ports to serve the massive loads required to operate in an emergency?

Smaller-scale microgrids that serve critical port functions (including support for force projection) offer a more viable near-term option than full-port projects. Some targeted initiatives employing IBRs are already underway. For example, the Port of Long Beach is paring a 300-kilowatt photovoltaic system with a 250-kilowatt BESS to power its main security facility, the Joint Command and Control Center, if the surrounding grid blacks out.[93] Over the longer term, emerging technologies could also make it possible to establish much larger power islands to keep major ports operating and—at least as important—sustain water systems, hospitals, and other facilities that are essential to public safety and societal continuity.

Defending the American People

Former CISA director Jen Easterly warned that China's deployment of Volt Typhoon malware against the grid and other infrastructure is aimed at "unleashing mass disruption on the US in the event of a major conflict to induce societal panic and deter our ability to marshal military might and citizen will."[94] Widespread societal panic, in turn, would intensify pressure on US leaders to abandon their defense of Taiwan or other regional partners, especially if the loss of power to thousands of water and wastewater systems, hospitals, and other facilities posed dire threats to public health and safety. Moreover, while Volt Typhoon poses an especially severe threat to such systems, Easterly cautioned

[88] Bell, "Installation Resilience, Combat Readiness."

[89] Lawrence, "Military Is Turning to Microgrids."

[90] Port of Los Angeles, "Facts and Figures."

[91] Idso et al., *Port Electrification Handbook*.

[92] My thanks to Steve Naumann (former Exelon Corporation vice president responsible for transmission and NERC policy) for calling this problem to my attention.

[93] Port of Long Beach, "Microgrid Project."

[94] CISA, "Easterly's Remarks."

that it is "likely just the tip of the iceberg" and that "there is, we believe, much we are not seeing."[95]

Dispersed generation can help strengthen public safety and societal resilience against PRC attacks. Many hospitals, emergency operations centers, and other lifeline facilities have emergency generators and enough diesel fuel stored on-site to operate for at least a few days without needing resupply. Hydrogen fuel cells and other advanced backup systems are creating new opportunities to serve such loads.[96]

In addition, by deploying microgrids that pair DERs with increasingly long-duration energy storage systems, these facilities may be able to significantly extend their ability to operate independently of the grid. Multiple large-scale microgrids that serve neighboring facilities can offer further advantages of efficiency and resilience. For example, San Diego Gas & Electric already operates twenty microgrids rated at ninety-five megawatts and has another two hundred-plus megawatts in development, all of which can function independently of or in parallel with its large regional transmission and distribution system.[97]

Technological advances are also enabling new options for serving multiple high-priority facilities across wide areas when BPS blackouts occur. The Electric Power Research Institute is developing ways to form emergency "energy pathways" that connect DERs to critical loads while isolating them from the surrounding system, utilizing solar, storage, and other resources wherever they naturally exist and reconfiguring the grid to create pathways, effectively routing energy to where it is needed most.[98]

Opportunities are also emerging to drastically increase the size of microgrids and create wide-area power islands. For example, AI tools can help grid operators plan for and execute the segmentation of large islands from the surrounding grid (and manage power flows within those islands) much more effectively than has been possible in the past.[99] Advances in control systems and other technologies may also enable large-scale microgrids to feed power to the BPS and help limit instabilities when the grid is under attack (and, ideally, obviate the need for segmentation).[100] And for the still longer term, DOE and the National Renewable Energy Laboratory are exploring how networked microgrids might serve as building blocks to strengthen the resilience of the US electric system as a whole.[101]

Anticipating PRC Countermeasures

Sharply increasing the number and scale of microgrids and larger power islands will create complex problems for grid reliability and security. One issue: if thousands of microgrids (or a few massive power islands) simultaneously segment from the BPS, that process could create widespread frequency and voltage disturbances and inadvertently help the PRC achieve its goals.[102] Initiatives to leverage the potential security benefits of DER-based microgrid expansion must be closely coordinated with measures to strengthen the reliability of the BPS and that system's resilience against PRC cyberattacks.

[95] Vicens, "Potential Chinese Cyberattack."

[96] DHS, "Using Hydrogen to Power Disaster Relief."

[97] Wolf, "Microgridation."

[98] EPRI, *SOLACE*.

[99] Mohammadi et al., "Artificial Intelligence Techniques in Microgrids"; and Walton, "Artificial Intelligence."

[100] Safder et al., "Microgrid Stability and Energy Management."

[101] Donde et al., *Microgrids as Building Blocks*; and Liu et al., *Building Blocks for Microgrids*.

[102] The US "grid is designed to operate at a frequency of 60 hertz (Hz). Deviations from 60 Hz can have destructive effects on generators, motors, and equipment of all sizes and types. . . . Voltage must be controlled to protect system reliability and move power where it is needed in both normal operations and following a disturbance" (NERC, *Essential Reliability Services*, 2).

China may also directly target microgrids for disruption. Indeed, as their accelerating construction helps secure fort-to-port operations and public safety, they will become increasingly high-value targets. DOD, DOE, and state governments are encouraging new microgrid deployments.[103] However, as with grid modernization in general, these deployments are going forward without an equivalent build-out of security mandates to defend them.

DOD exemplifies this gap. While the US Army and other services are building hundreds of microgrids, none of those plans include requirements to secure the IBRs or energy management systems the projects incorporate. Nor has the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment or any other DOD component provided microgrid-specific cybersecurity mandates, beyond the general policies and guidelines offered by the Installation Energy facility-related control systems (FRCS) cybersecurity guide and related documents.[104]

Given the growing importance of microgrids for defense against China, the department should issue specialized guidance to strengthen their cyber resilience and counter the specific threat vectors examined later in this study, especially the deployment of Chinese-produced software and hardware. State regulators should establish similar security mandates for microgrids under their jurisdiction that serve major hospitals, water systems, and other societally vital facilities.

Decentralized Power Restoration

If a Far East conflict with China extends for weeks or months, the PRC will seek not only to expand the geographic scope of US power outages but also to extend their duration. That possibility will put a premium on the ability of transmission system operators (TOPs) and their partners to rapidly restore power amid sustained cyberattacks against them.[105] In past US outages, TOPs have almost always restored power from the outside in—that is by importing power to a blacked-out region from unaffected generation and transmission assets on its perimeter. In addition, TOPs have the ability to perform inside-out restoration, restarting the grid from within a blacked-out area without relying on external sources of power. That "blackstart" capability will be vital if the PRC is able to inflict multiregional or even nationwide outages.

Grid decentralization will enable the United States to achieve an especially valuable "twofer": resilience against both cyber and kinetic threats.

Extensive NERC requirements are structured to help ensure that TOPs are able to meet the complex, technically difficult challenges that blackstart operations entail.[106] NERC's cybersecurity standards also apply to systems and facilities critical to system restoration, including blackstart resources.[107] Yet, NERC rates these systems as "low impact," the category that carries the least stringent cyber protection requirements. NERC, reliability coordinators, and other BPS entities reassessed that low ranking in 2023 and identified a number of reasons to retain it.[108] Given the increasing importance of survivable blackstart capabilities vis-à-vis the PRC, and the resulting likelihood that the PRC will prioritize blackstart systems for disruption, NERC should recategorize those systems as high impact and strengthen their security requirements

[103] Nilsson, "US Microgrid Market to Grow"; and Ferreira et al., *DOE 2021 Strategy White Papers on Microgrids*.

[104] DOD, "FRCS Cybersecurity" and "Managing Cyber Risks."

[105] TOPs are the entities responsible for the reliability of their "local" transmission systems and that operate or direct the operations of the transmission facilities. NERC, *Glossary*, 43.

[106] NERC, *EOP-005-3*. For additional standards, refer to NERC, "Project 2006-03."

[107] NERC, *CIP-002-6*, 7.

[108] NERC, *CIP-002-6*, 19.

accordingly.[109] TOPs should also continue to implement lessons learned from Defense Advanced Research Projects Agency programs to strengthen blackstart resilience.[110]

At the same time, TOPs should press forward on a structural opportunity to bolster blackstart resilience. These system operators currently rely on a small number of dedicated "cranking paths" to restart the grid from within blacked-out areas. And while they typically have restoration backup plans and capabilities to employ if their primary cranking path is disrupted, the centralized structure of blackstart infrastructure today makes it easier for the PRC to map and concentrate attacks against those assets and operations.

The widespread deployment of BESS and advanced inverters may enable TOPs to decentralize their systems and employ a far more dispersed set of blackstart generation resources and starting points for restoration.[111] For batteries to play this role, however, they will need to be equipped with GFM inverters that have only recently been deployed and still need technical refinements.[112] Managing the restoration process with highly dispersed blackstart resources, and balancing generation with load as decentralized restoration goes forward, will pose still greater challenges. Recent field tests by the UK National Grid Electricity System Operator demonstrated significant progress in meeting these operational requirements and effectively employing DERs for system-wide restart.[113] If TOPs, reliability coordinators, and their partners can overcome the many remaining impediments to decentralized restoration, the United States could shift to a system that could be much more difficult to target and disrupt.

Multi-Hazard Resilience

An extraordinary confluence of natural and human-made hazards is challenging the grid's resilience—that is, "the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions."[114] Strategies to strengthen cybersecurity must account for the competing funding demands that these hazards can entail, especially given the priority of state regulators and FERC to keep electricity affordable.

Regulators and the electric industry must also guard against the danger that measures optimized to address one challenge will intensify others. Indeed, to the maximum extent possible, these partners should pursue initiatives that provide benefits against multiple hazards.

Russia's efforts to destroy Ukraine's electric system highlight the potential benefits of grid decentralization against airborne threats.

Grid decentralization offers just such an opportunity. DER-enabled microgrids have long allowed facilities to sustain their critical functions when confronted with hurricanes and other severe weather events. The deployment of advanced DER inverters is also helping sustain power flows in the face of intensifying wildfires and other consequences

[109] Compliance with more stringent security requirements will impose costs on blackstart resource providers. To incentivize providers to continue to provide assets for blackstart, regulators will need to fully compensate them for those additional expenses.

[110] DARPA, "RADICS."

[111] Stockton et al., *Blackstart Power Restoration*. GFM inverters and IBR-enabled blackstart opportunities are examined in greater detail in Appendix A.

[112] For a definition of GFM inverters and a summary of their potential power restoration roles, see NERC, *Grid Forming Technology*, iv, 16. A cranking path is "a portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units" (NERC, *Glossary*, 11).

[113] National Grid ESO, *Distributed ReStart*.

[114] White House, NSM-22.

of climate change. Now, for defense against PRC attacks, grid decentralization will enable the United States to achieve an especially valuable "twofer": resilience against both cyber and kinetic threats.

While multiple high-powered rifle attacks against selected BPS substations could have significant regional effects, still greater consequences could result from coordinated strikes by advanced UASs. The Chinese company DJI produces nearly 80 percent of drones purchased by US consumers.[115] CISA warns that such Chinese-made UASs "pose a significant risk to critical infrastructure and U.S. national security."[116] In November 2024, the Department of Justice charged a domestic extremist with planning to conduct a drone attack on the grid.[117] Government–industry collaboration is now crucial to build resilience against more sophisticated, large-scale UAS attacks by the PRC or other nation-state adversaries.

Russia's efforts to destroy Ukraine's electric system highlight the potential benefits of grid decentralization against airborne threats. UAS attacks on our system would differ from those in Ukraine. Russia launches and operates very large UASs (including the Shahed-136) from its own territory for cross-border strikes. Potential US adversaries will lack that geographic advantage. But proximity will not be needed to employ large numbers of smaller, domestically launched UASs in coordinated attacks against critical substations, especially as those systems acquire increasingly sophisticated autonomous control capabilities.[118]

Our utilities are poorly prepared to defeat such attacks. To comply with NERC Standard *CIP-014-1—Physical Security*, BPS entities are protecting substations and other assets with increasingly effective ballistic fencing and other barriers.[119] However, fences are useless against UASs that fly over them to destroy substation equipment. NERC should prioritize the development of standards against airborne threats. The Federal Aviation Administration, which is testing UAS detection and mitigation systems at US airports, should also partner with other agencies and utilities to develop and authorize counter-UAS options to protect high-impact grid assets.[120] In addition, the administration and Congress should establish a broader strategy to defeat UAS attacks on other key infrastructure nodes within the United States and to build on the authorities that DOD base commanders already have to defend their installations from such airborne systems.[121]

BPS and distribution utilities can also draw on Ukraine's response to Russian UAS and missile attacks. Volodymyr Kudrytskyi, chief of Ukraine's state-owned grid operator, says Ukraine needs to move away from its reliance on a handful of very large, easily targeted power generators. Kudrytskyi states that "the only way to build a sustainable, safer, and more resilient energy system protected from enemy attacks is to construct 200 power plants of 5 MW each instead of one 1000 MW power plant."[122] Maxim Timchenko, the head of another major Ukrainian utility, noted that solar farms can recover from damage far more quickly than thermal generation plants. The resulting benefits for power resilience constitute "the difference between centralized and so-called decentralized generation. It's much more resistant and difficult to destroy."[123] Together with measures to decentralize Ukraine's transmission and distribution systems, transition to centralized small-scale gas turbines,

[115] Kashgar, "Drone Maker Expands."

[116] CISA, *Chinese-Manufactured UAS*.

[117] DOJ, "Man Arrested and Charged."

[118] Naumann, *Threat to the Electric Grid*.

[119] NERC, *CIP-014-1*.

[120] FAA, "UAS Detection and Mitigation Systems Aviation Rulemaking Committee."

[121] Barnes, "Mystery Drones."

[122] Mukhina, "Decentralized Generation Network."

[123] Prengaman, "Clean Energy."

and construct microgrids for hospitals and other critical facilities, energy officials are restructuring Ukraine's electric system as a whole to make it more survivable against UASs, as well as missiles and hypersonic weapons.[124]

Grid decentralization will offer the United States equivalent benefits for resilience against coordinated UAS strikes, as well as attacks with high-powered rifles, high explosives, and other kinetic means. Reducing the potential effectiveness of hypersonic strikes will be valuable over the longer term. China and Russia are rapidly improving their capabilities to strike US territory with conventionally armed hypersonic weapons.[125] Of course, initiating such attacks against the US grid or other targets would carry massive punitive and escalatory dangers. Nevertheless, in addition to convincing foreign leaders that hypersonic strikes would incur costs they would find unacceptable, the United States should seek to reduce the benefits that those leaders expect to achieve by attacking. That brings us to the most audacious (and, if achieved, most valuable) goal for restructuring the US electric system: bolster deterrence against attacks and thereby make them less likely.

Shaping the Enemy's Calculus of Benefits and Costs

The 2022 National Defense Strategy calls for measures to strengthen "deterrence by denial" and "deterrence by resilience." Such measures should reduce the adversary's "expected benefits for aggressive action against the homeland," including attacks on infrastructure, while DOD at the same time takes steps to increase the "direct and indirect costs" potential attackers would suffer as a result of US response operations.[126]

Many of the initiatives recommended in this section offer value to both sides of this equation. Microgrid initiatives, decentralized power restoration, and other measures will not only help counter Chinese goals of disrupting US power projection and inciting societal panic but will also help ensure that our military bases (and the off-base water systems and employee housing on which they depend) have the electricity they need to respond to PRC attacks, even if attacks continue for weeks or months.[127]

Different deterrent postures may be needed against Russia or other adversaries. The National Defense Strategy also emphasizes that initiatives to sustain and strengthen deterrence should be tailored to specific competitors. A pioneering study by the Defense Science Board notes that "because deterrence operates by affecting the calculations of specific decision-making individuals in another nation or group—the goal being to convince these decision makers that the expected costs of an attack outweigh its expected benefits—deterrence planning must focus on what key leaders on the other side value, and on how they are likely to make decisions."[128]

The need for such tailoring is greater for cost imposition than deterrence by resilience. Shaping the grid's decentralization to maximize its survivability against cyber and kinetic weapons will be valuable regardless of who attacks. The same is true of hardening distributed digital grid assets and communication networks against electromagnetic pulse effects and other potential common-mode failures.

Strengthening deterrence by resilience also entails a monumental problem. While the United States

[124] Stern, "Being Rebuilt Green." Of course, if Russia continues to ramp up the scale of its missile attacks against Ukraine's electric system, even a highly distributed system will eventually be overwhelmed.

[125] Seldin, "China Is Leading in Hypersonic Weapons."

[126] DOD, *2022 National Defense Strategy*, 8–9.

[127] On the imperative to focus grid resilience investments on such defense installations, see DOD DSB, *Task Force on Cyber Deterrence*, cover memorandum for study.

[128] DOD DSB, *Task Force on Cyber Deterrence*, 10.

has barely begun to leverage grid restructuring for national security, China and other potential adversaries have been exploiting our shift to digitized, distributed resources for years. As DOE warns, "attackers are evolving their practices and capabilities against new technology faster" and are "positioned well to enter DER energy systems."[129]

Securing the Grid against Supply Chain Exploitation

Embedding compromises in DER systems is dead easy if you manufacture them. Ninety percent of the inverters sold in the United States are made in or source parts from the PRC.[130] We already know that PRC companies with close ties to the People's Liberation Army (PLA) have covertly embedded cellular modems in cranes deployed in US seaports.[131] Chinese manufacturers also have immense opportunities to penetrate the devices they sell to providers of power to those ports and to critical civilian and military customers nationwide.

In its 2022 report *America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition*, DOE warned that supply chain risks to the sector "have grown in recent years as increasingly sophisticated cyber adversaries have targeted and exploited vulnerabilities in these digital assets." The authors go on to say:

> Key cyber vulnerabilities include reliance on untrusted foreign suppliers and software developers; reliance on opaque and highly dynamic global supply chains for digital goods and services; high and often unrecognized reliance on certain ubiquitous key digital components in energy sector systems that have the potential for cascading effects if concurrently compromised; and fragmentation and inconsistent oversight of interdependent of cyber supply chains.[132]

DOE also identifies multiple ways that adversaries can employ compromised devices to create outages. Attackers can add "backdoor capabilities that permit unauthorized access and control"—they can "leverage trusted supplier relationships to plant backdoors, weaken security measures, and change the underlying functionality of legitimate software to suit their needs."[133] Supply chain attacks can also occur over multiple phases in the life cycle of a device. Adversaries can "compromise a development environment to taint new software as it comes out of production or compromise authorized updates for software or hardware already deployed."[134] Sophisticated adversaries may also "add a chip onto the printed circuit board design that duplicates data in memory and sends it to the attacker, giving the attacker credentials and login data to the compromised devices."[135]

Grid decentralization will not diminish the severity of such threats. DOE warns that as distributed resources grow and are increasingly interconnected with the BPS, the simultaneous exploitation of compromised DERs could create cascading losses of power and—in severe attacks—a "complete blackout."[136] In addition, "compromised DER settings could obscure the actual operational state of DER and, in sufficient number, cause grid voltage and current violations. Attacker execution of compromised configurations also would lead to DER not responding to distributed energy resource

[129] DOE, *Cybersecurity Considerations*, 16.

[130] DOE, *Battery Energy Storage Systems*, 11.

[131] HCHS, "Shocking Findings." On measures now underway to address these and other threats, see White House, *Initiative to Bolster Cybersecurity of U.S. Ports*.

[132] Igogo et al., *America's Strategy*, 41–42.

[133] DOE, *Cybersecurity Considerations*, 14.

[134] DOE, *Cybersecurity Considerations*, 15.

[135] DOE, *Cybersecurity Considerations*, 15.

[136] DOE, *Cybersecurity Considerations*, 22.

management system (DERMS) control requests and impacting DER provision of grid services."[137]

DOE is partnering with suppliers and manufacturers to counter these threats to energy supply chains. Its 2024 Supply Chain Cybersecurity Principles, supported by Schweitzer Engineering Laboratories, Schneider Electric, and other major product providers, offer especially valuable guidelines to strengthen supply chain security.[138]

Nevertheless, the scale of the threat is immense. DOE has not publicly described the extent to which such compromises are embedded in the grid. However, a December 2023 private-sector report on grid software supply chains highlights the increasing severity of such threats. Using software bill of materials (SBOM) data, analysts found that 90 percent of the software products used to manage the US electric system contain code "contributions" from Chinese or Russian developers, many with critical vulnerabilities that could enable subsequent exploitation.[139]

Under the Made in China policy, the PRC has made the development, production, and international sale of energy equipment a top priority.

China as the Pacing Threat to Grid Supply Chains

As exemplified by the Russian Foreign Intelligence Service's SolarWinds attack, which victimized 25 percent of electric utilities, Russia has sophisticated capabilities to insert backdoor code and achieve other supply chain compromises.[140] However, China enjoys an advantage that Russia lacks: the heavy dependence of the US grid's modernization on Chinese products. That dependence is no accident.

Under the Made in China 2025 policy adopted by China's State Council in 2015, the PRC has made the development, production, and international sale of energy equipment a top priority for achieving global economic leadership.[141] Within that priority, "clean energy" hardware and software, including solar and wind system components and their digital control systems, are particular areas of emphasis. China's *14th Five-Year Plan for Energy Technology Innovation* (2021) targets digital energy technologies and calls for maintaining an 80 percent share of global renewable energy equipment production.[142]

With the grid's accelerating transformation and the deployment of millions of new BESS, solar and wind assets, and associated control systems, scores of Made in China companies are exploiting this growth.[143] In fact, a number of US states have explicitly approved their distribution systems' purchasing of Chinese-produced inverters and other digital energy products, even in areas where the PLA is most likely to interfere with US force deployment.

California and Hawaii exemplify these problems. Press accounts report that hackers affiliated with China's PLA burrowed into the computer systems of about two dozen critical entities during 2023, including infrastructure systems in Hawaii and the West Coast, as well as in Guam and other areas crucial for deploying forces to potential conflicts

[137] DOE, *Cybersecurity Considerations*, 22.

[138] White House, *Statement from National Security Advisor Jake Sullivan*; and DOE, *Supply Chain Cybersecurity Principles*.

[139] Fortress Information Security, *Software Supply Chain*.

[140] FERC and E-ISAC, *SolarWinds and Related Supply Chain Compromise*; and Walton, "Growing ICS Vulnerabilities."

[141] Sutter, "*Made in China 2025*."

[142] Sandalow et al., *Guide to Chinese Climate Policy 2022*; and Howe, "China's Renewable Energy Boom."

[143] Made-in-China, "Inverter."

in the Taiwan Strait.[144] Yet, the California Energy Commission's Solar Equipment Lists, which identify the inverters and other digital equipment that meet "established national safety and performance standards," include a dozen Chinese companies (and hundreds of individual products).[145] Furthermore, no state or federal security mandates exist to exclude these products from California's approved list, regardless of the severity of their risks to the grid and US force projection.

Hawaiian Electric Company has an equivalent list of inverters and controllers approved for interconnection to its infrastructure. Again, the list includes multiple Chinese companies, allowing them to embed their products in the electric systems that serve Joint Base Pearl Harbor-Hickam, Honolulu Harbor, or other facilities that will be essential for DOD in potential regional conflicts with the PRC.[146] A further problem: in accordance with the Federal Power Act, Section 215(k), NERC supply chain standards and other security mandates do not apply to Hawaii's high-voltage system.[147]

Countering the Threat

Existing supply chain risk management (SCRM) initiatives provide a foundation for progress. BPS entities must comply with *CIP-013-2—Cyber Security—Supply Chain Risk Management,* which establishes security controls for managing risks to cyber systems' supply chains.[148] However, in September 2024, FERC found that "although the currently effective SCRM Reliability Standards provide a baseline of protection against supply chain threats, there are increasing opportunities for attacks posed by the global supply chain."[149] FERC goes on to say that existing standards "do not provide specific requirements as to when and how an entity should identify and assess supply chain risks, nor do the Standards require entities to respond to those risks identified through their SCRM plans." This "could lead to an entity installing vulnerable products and allowing compromise of its systems . . . 'effectively bypassing security controls established by CIP Reliability Standards.'"[150] FERC has proposed to direct NERC to submit new or modified standards to fill these gaps.

Fortunately, many BPS entities not only comply with NERC standards but also voluntarily adopt more stringent measures. Industry associations help them do both. In coordination with NERC, the North American Transmission Forum (NATF) and other electric industry organizations are also offering detailed guidelines to help utilities manage supply chain risks.[151] State regulators are driving SCRM improvements at the distribution level as well, by leveraging BPS best practices, NARUC research and recommendations, and DOE's Cybersecurity Capability Maturity Model.[152]

Utilities are also employing SBOMs to help their procurement officers assess the degree of risk posed by potential software purchases. Executive Order 14028, *Improving the Nation's Cybersecurity*, defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software."[153] NIST has provided a series of recommendations for using

144 Nakashima and Menn, "China's Cyber Army."

145 California Energy Commission, "Solar Equipment Lists Program" and "Solar Equipment Lists."

146 Hawaiian Electric, "Qualified Grid Support." It is possible (and highly desirable) that nonpublic measures are underway to bar the use of high-risk Chinese products from defense critical electric systems in Hawaii and elsewhere.

147 The Federal Power Act also excludes Alaska from such BPS standards (16 U.S.C. § 824o - Electric Reliability).

148 NERC, *CIP-013-2*.

149 FERC, *Supply Chain Risk Management Reliability Standards Revisions*, 2.

150 FERC, *Supply Chain Risk Management Reliability Standards Revisions*, 19–20 (and quoting FERC, *2023 Lessons Learned*, 17–19).

151 NATF, "Industry Organizations Collaboration."

152 Muneer et al., *Cybersecurity Capability Maturity Model*.

153 Exec. Order 14028, § 10(j).

SBOMs to increase transparency, provenance, and the speed at which vulnerabilities can be identified and remediated by federal departments and agencies.[154] Supported by CISA, a growing number of utilities are also exploring the use of hardware bills of materials to help them assess the security risks posed by untrusted or compromised components of grid devices and equipment.[155]

It would be foolish, however, to rely on Chinese manufacturers and software developers to fully itemize the components of their products in response to utility-issued requirements for bills of materials (software or hardware). China, Russia, and other adversaries may also use subterfuge to introduce compromised subcomponents into equipment and software sold by US and allied companies, inserting backdoors or additional exploits of which those companies are unaware.[156] Effective SCRM will require sophisticated product assessment tools that can detect compromise in the face of these complexities and the opportunities for adversary penetration they create.

Utility procurement officers and manufacturers also need to address the risk posed by subcomponent providers. If grid owners can choose from a diverse array of inverters and other hardware, firmware, and software products that are sold by multiple companies, the PRC's efforts to compromise and exploit US supply chains will be more difficult than if it needs to penetrate only a handful of providers. The benefits of heterogeneity vanish, however, if many of these products incorporate subcomponents (or sub-subcomponents) provided by Chinese companies. Identifying these "third-party" providers and assessing their risks to the final product's security poses an immense challenge for utilities, especially if the PRC uses subterfuge to hide its contributions. One power company executive states that "my third-party assessments are up over 300 percent, year after year," and the expertise to conduct them is "hard to find." Moreover, they note that "in the renewables space, it gets 'very China very fast,' so understanding three or four layers down in the manufacturing supply chain is critical" to identify cyber vulnerabilities.[157]

Product Testing

Only the largest utilities have the expertise to analyze digital devices at the chip level to identify covert software exploits. Many distribution utilities, as well as aggregators and other new participants, have no such analytic capabilities and will never be able to afford them. To provide the full range of grid operators with detailed information on product risks, DOE and its national laboratories should scale up their current programs to analyze potentially dangerous products.

The Idaho National Laboratory (INL) CyTRICS (Cyber Testing for Resilient Industrial Control Systems) program exemplifies the value of such work. Under CyTRICS, INL partners with multiple national laboratories, manufacturers, and other resilience stakeholders to

- identify high-priority operational technology (OT) components/systems;
- test those systems to identify potential compromises;
- share information about supply chain vulnerabilities; and
- support improvements in component design and manufacturing.

CyTRICS applies threat intelligence; identifies common-mode vulnerabilities in high-impact hardware, software, and firmware; and responsibly discloses identified vulnerabilities to manufacturers and asset owners, who can act to address the

[154] NIST, "SBOM."

[155] CISA, *HBOM Framework*.

[156] Caddy et al., *Cybersecurity and Digital Components*, 6–7.

[157] Private communication with the author.

weaknesses before adversaries can exploit them. The program also maintains a central data repository that stores bills of materials from testing for cross-component and impact analysis. That repository enables rapid identification of high-risk subcomponents and sector-wide analysis of systemic dangers.[158]

DOE, INL, and their private-sector partners should expand the CyTRICS program to handle the flood of Chinese inverters and other products now being deployed on the US electric system and ensure that utility procurement officers are told which of these products are compromised. The problem: thus far, manufacturers that partner with CyTRICS to analyze their products do so on a voluntary basis. Few Chinese manufacturers, especially those closely allied with the PLA or Chinese Communist Party (CCP), are likely to request such scrutiny. Other, non-collaborative, approaches will be needed to select and analyze high-risk products from the PRC.

Ongoing efforts to expand the CyTRICS program's throughput could help meet such requirements. INL states that it is producing a standardized approach to vulnerability testing and subcomponent enumeration for hardware, software, and firmware, which will enable the "scale up of testing beyond DOE National Laboratories to industry partners."[159] In addition, a rapidly growing number of SCRM assessment companies provide fee-based services to assess product security, provide data libraries, and collaborate with willing US and allied manufacturers to remediate vulnerabilities and exploits. DOE should actively support such initiatives and—with appropriate licensing and security arrangements—*immediately* transfer CyTRICS assessment technologies to private-sector partners so they can scale up testing.

If we classify data on high-risk products, that information will not reach the thousands of aggregators and other component purchasers who lack security clearances.

Data Sharing

DOE needs to revamp its system for sharing SCRM information across the electricity subsector. Data confidentiality, liability concerns, and other factors currently impede distribution of information on compromised components. Classification of sensitive data poses an especially thorny problem. If we broadly share the finding that a particular product has been found to be compromised, the PRC might use the information to assess our testing methods and design future compromises to maneuver around those capabilities. But if we classify data on high-risk products, that information will not reach the thousands of aggregators and other component purchasers who lack security clearances.

The deployment of Chinese-produced BESS exemplifies the imperative to improve information sharing. Fujian-based CATL is the world's largest manufacturer of lithium-ion batteries, which are used for microgrids, hybrid power plants that combine IBR generation with storage, and EVs (including those employed by Tesla and General Motors). CATL batteries have already been installed in hybrid plants in Florida, Virginia, Nevada, and California, as well as in a solar farm operated by Duke Energy–leased land inside Camp Lejeune. CATL is closely aligned with the CCP and maintains a CCP cell within its organization.[160]

[158] INL, "CyTRICS" (fact sheet). CyTRICS is also the central component of the new Energy Cyber Sense program (per § 40122, FY22 Infrastructure Investment and Jobs Act), which integrates DOE cyber supply chain programs. The Biden administration also called for measures to leverage CyTRICS and existing technical assistance programs to identify and assess vulnerabilities in linchpin technologies and capture lessons learned for penetration testing (White House, *Enhancing the Digital Ecosystem*).

[159] INL, "CyTRICS" (fact sheet).

[160] Singleton, *Beijing's Power Play*.

In December 2023, then-Senator Marco Rubio (R-FL) and other legislators sent a letter asking the secretary of defense to "immediately reverse" the installation of CATL batteries at Marine Corps Base Camp Lejeune, North Carolina. Duke Energy then disconnected the batteries.[161] In January 2025, DOD blacklisted CATL from receiving Defense Department contracts after May 2026.[162] That decision sends an implicit signal that the company's batteries threaten national security. But neither DOD nor DOE, nor any other federal agency, followed up with public guidance as to whether CATL batteries do indeed contain compromises or other features that China could use to disrupt or manipulate power flows. Such explicit notifications are essential if procurement officers are to balance the benefits of low CATL prices against the supply chain dangers they entail.

A number of government and industry organizations are addressing these data-sharing challenges and providing unclassified but valuable SCRM data to utilities under the Traffic Light Protocol (TLP) system—including TLP:RED information that is subject to special protections against unauthorized release.[163] The Electricity Information Sharing and Analysis Center (E-ISAC) is especially notable in this regard. Established in 1999 and operated by NERC, the E-ISAC serves as the clearinghouse for electric industry security information, distributing information, including on supply chain threats, to utilities.[164] The E-ISAC is also part of the newly established Energy Threat Analysis Center (ETAC), a DOE-led initiative that features collaboration between electric industry partners and government agencies through the DHS CISA Joint Cyber Defense Collaborative. The ETAC will serve as a spoke to the Joint Cyber Defense Collaborative hub and enable operational intelligence collaboration for the entire energy sector.[165]

Industry associations are helping utilities gain expanded access to product data and employ risk management models. For example, NATF provides BPS entities with a Supply Chain Security Assessment Model to help them evaluate vendor supply chain security practices. The model also helps its users comply with NERC supply chain reliability standards.[166] NATF's program provides a model that NARUC might adapt to meeting distribution entity needs, especially as states develop new interconnection requirements and other standards to ensure that safer products are deployed.[167] Publications by industry experts on SCRM are useful as well.[168]

In addition, the National Security Agency (NSA) is expanding its information-sharing programs to support private-sector SCRM. The Enduring Security Framework provides threat data to companies in the defense industrial base, communications, and information technology sectors, including infrastructure owners and operators, as well as products on software supply chains and other threat vectors. NSA products also offer recommendations to mitigate such threats.[169] The NSA should expand these collaborative efforts to include electric utilities, especially those that China is likely to

[161] Martina, "CATL Batteries."

[162] DOD, *Designation of Chinese Military Companies*. Previous actions to restrict the use of DOD funds to purchase batteries produced by CATL and other designated companies were provided by the National Defense Authorization Act for Fiscal Year 2024, § 154.

[163] The TLP system is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipients, ranging from red (not for disclosure, restricted to participants only) to green (limited disclosure, restricted to the community) (CISA, *Definitions and Usage)*.

[164] *Examining Emerging Threats* (testimony of Manny Cancel).

[165] *Examining Emerging Threats* (testimony of Manny Cancel).

[166] NATF, *Supply Chain Security Assessment Model*.

[167] Refer to Lyu and Xie, *Inverter-Based Resource Interconnection Standards*, for a comprehensive review of such interconnection standards.

[168] Crossley, *Software Supply Chain Security*; and Hughes and Turner, *Software Transparency*.

[169] NSA, *2023 NSA Cybersecurity Year in Review*.

target to disrupt fort-to-port operations and other defense missions.

DOE and its partners should also expand utility personnel's access to classified information on compromised products they are deploying (or considering for purchase). For years, utilities and their advocates in Congress have pressed DOE to increase the number of security clearances it provides to grid operators.[170] If the department and its Intelligence Community partners determine that it is crucial to prevent adversaries from knowing that their compromises have been identified yet still enable utilities to make risk-informed decisions on those products, growing the number of cleared, carefully vetted personnel in the electric industry will be necessary. The use of one-day read-ins to provide temporary access to classified data should also be expanded. In both cases, however, DOE and its partners must balance the security benefits of such measures against the dangers of expanding the pool of cleared personnel, all of whom will be targets for human intelligence espionage and potential adversary recruitment.

Voluntary Guidelines and (As Needed) Prohibition Orders

It would be impractical to immediately ban the sale of all Chinese hardware and software to US utilities. Thanks to China's strategies to exploit the US grid's transformation, including by subsidizing solar, wind, and battery manufacturers to undercut US competitors, the dependence of many American grid operators on Chinese products is too deep and pervasive to go "cold turkey."[171] It is even less plausible that Congress will require utilities to rip out all Chinese products from their electric systems and replace them with safer but more expensive alternatives from US or allied sources. The cost and difficulty of doing so would be immense.

Instead, as noted above, we need a risk-based approach to constrain—and, if necessary, prohibit—the deployment of those Chinese products that pose the greatest danger to the US electric system. DOE's report *Strategy to Secure the Supply Chain* provides the starting point to do so. The strategy emphasizes that a "key" cyber vulnerability lies in the "high and often unrecognized reliance on certain ubiquitous key digital components in energy sector systems that have the potential for cascading effects if concurrently compromised."[172] Accordingly, the analysis below proposes how to focus SCRM initiatives on devices and control systems that (1) are being deployed nationwide as part of the grid's transformation; and (2) could be simultaneously exploited to create cascading outages and help Beijing achieve its goals in attacking the grid, including spurring societal panic and disrupting fort-to-port operations.

The Trump administration should rapidly issue prohibitions for especially high-risk products for both the BPS and distribution systems.

Voluntary measures will be adequate for low-risk products. The SCRM guidelines provided by DOE, NIST, NARUC, and private-sector organizations help grid operators meet the challenges such components pose, especially because many of these organizations continuously update their recommendations in response to the intensifying threat. Making product data available to procurement officers will also help utilities, aggregators, and VPP operators apply these guidelines to make specific purchases on a risk-informed basis rather than automatically selecting Chinese products because of their lower prices. And when utilities seek special tariffs or rate cases to recover their costs for buying

[170] Gheorghiu, "Utility Security Clearances."

[171] On Chinese state subsidies and strategic underpricing to undercut US competitors, see USCC, "China's Energy Plans and Practices," 263–267.

[172] Igogo et al., *America's Strategy*, 41–42.

safer but more expensive components, sharing supply chain threat data with regulators can help ensure that their requests will be approved.

More stringent measures will be needed for products that pose severe threats to the grid. As discussed above, mandatory BPS supply chain standards do not apply to local distribution companies or DER aggregators—the same grid operators that are rapidly purchasing the energy products prioritized for sale by Made in China. The solution: prohibit the purchase of the highest-risk products across the entire electricity subsector, including DERMS and other energy management systems that Beijing could use to create wide-area instabilities.

If domestic or allied sources of critical grid equipment are available, even if more costly than Chinese alternatives, prohibitions on the most dangerous projects offer an immediate way to manage grid risks. The telecommunications sector offers precedents to establish risk-based prohibitions. In December 2020, the US Federal Communications Commission (FCC) affirmed its determination that Huawei Technologies Co. "poses a threat to the security and integrity of our nation's communications networks or the communications supply chain."[173] The Biden administration subsequently banned the sale or import of telecommunications equipment from Huawei, ZTE, and other selected Chinese companies posing "an unacceptable risk" to US national security.[174] That prohibition provides a model for applying equivalent bans on dangerous grid products. So, too, could the Commerce Department's proposed prohibition of the sale or import of Chinese and Russian cellular, wireless, and other "connected" vehicles and components, which pose "acute threats" and could "undermine national security."[175]

An especially pertinent model lies in the prohibition order issued by the first Trump administration. On May 1, 2020, then-president Donald Trump issued Executive Order 13920, *Securing the United States Bulk-Power System*.[176] When the Biden administration rescinded the order in January 2023, DOE called for further analysis of supply chain mitigation options.[177] The second Trump administration should rapidly complete such analysis and issue prohibitions as needed for especially high-risk products for both the BPS and distribution systems and draw on lessons learned from the problems that have hobbled implementation of the order to rip and replace Huawei products under the Secure Networks Act.[178]

Making Grid Systems Secure by Design

Instead of relying solely on supply chain compromises, China can also strike the electric system by "living off the land" (LotL) and exploiting the intended functions and performance features of digital devices, energy management systems, and their supporting networks. CISA states that LotL attacks take advantage of built-in network administration tools and other network functions to enable system disruption. The advantage of this approach:

> The actor [can] evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations. . . . Many of the behavioral indicators included can also be legitimate system administration commands that appear in benign activity.[179]

[173] FCC, *Huawei Designation*, 2.

[174] Bartz and Alper, "U.S. Bans."

[175] White House, *Countries of Concern*.

[176] Exec. Order 13920.

[177] DOE, *Revocation*, 3.

[178] DOE, *Battery Energy Storage Systems*, 77–78.

[179] CISA, "Alert Code AA23-144a." For similar NSA assessments, see Starks, "Stealthy and Off-Limits Hacks."

LotL campaigns also enable adversaries to stay hidden in infrastructure networks for months or even years. The PRC's Volt Typhoon campaign exemplifies these advantages. CISA and its Intelligence Community partners found that Volt Typhoon achieved "long-term, undiscovered persistence" across IT systems of "multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and noncontinental United States and its territories, including Guam." CISA found indications "of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years."[180]

Once PRC attackers are embedded in IT networks, they can establish access in OT systems that control the grid and other infrastructure systems. CISA and its partners "assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions." Moreover, given the persistent presence that such LotL threats provide, CISA is "concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts."[181]

Industry and government progress is underway to counter these threats. CISA's Secure by Design initiative offers valuable guidelines to protect software and digital systems from adversary penetration and exploitation. Together with DOE's *National Cyber-Informed Engineering Strategy* and the product design components of its *Supply Chain Cybersecurity Principles,* NIST's *Cybersecurity for Smart Inverters*, and other government and industry guidance, manufacturers can apply a far-reaching set of recommendations to secure their products from LotL attacks.[182]

[180] CISA et al., *Joint Cyber Advisory*, 8, 2, 3.

[181] CISA, "Alert Code AA24-038A."

[182] McCarthy et al., *Cybersecurity for Smart Inverters*.

Yet, the grid's transformation is making the application of these principles more difficult. As the electric system becomes increasingly reliant on DERs and IBRs, inverters will need to provide sophisticated new capabilities to help maintain the system's reliability. Those same performance features will give adversaries a smorgasbord of new attack surfaces and opportunities to create multiregional blackouts.

From Spinning Mass to Digital Control

Conventional BPS generation assets, including fossil-fueled generators as well as hydro and nuclear power plants, are well suited to support reliability. They produce steam, create hot gas (in the case of gas- or oil-fired peaking units), or use flowing water to spin turbines that generate electricity. These spinning turbines and other rotating machinery, in turn, provide inertia for the electric system that helps maintain and restore the grid's stability when disturbances occur, including frequency droops and voltage transients (i.e., spikes or sudden decreases in voltage).[183] Natural gas and hydro generators are also capable of rapidly increasing or reducing their power output to help grid operators balance generation with changing loads, providing valuable ramping services for grid reliability.

The grid's increasing dependence on DERs and IBRs requires new ways to provide these reliability benefits. In contrast to conventional generation systems, these inverter-controlled resources do not employ rotating turbines and cannot provide the system inertia that has traditionally helped limit the impact of grid disruptions (including the loss of power plants or transmission lines) on grid frequencies. Conventional generators also offer additional capabilities for frequency control, including "governor actions" that rapidly sense changes in

[183] Muelaner, "Grid Frequency Stability"; and NERC, *Balancing and Frequency Control*.

local system frequency and automatically adjust the energy output of the resource to counteract those changes. These capabilities (known as primary frequency response) have long been of foundational importance to US electric system reliability.[184]

Some well-established technologies can help respond to disturbances as coal and other conventional generators go out of service. For example, with increased solar and wind deployments, synchronous condensers and additional flexible alternating current transmission system (FACTS) devices are being modernized and widely deployed as well to help respond to system disturbances.[185]

Yet, even with these developments, maintaining the grid's reliability will require us to follow an additional path: deploy increasingly "smart" inverters and other power electronics that enable solar, wind, and battery energy storage systems to provide the frequency support, voltage regulation, and other ERSs that conventional generators have traditionally provided.[186]

IEEE standards are helping drive such deployments. IEEE 1547-2018 and related standards specify minimum technical interconnection and interoperability requirements for DERs connected to the distribution system, including the ability to provide (1) continued power when disturbances occur and (2) autonomous response to voltage and frequency changes to support the grid, including voltage regulation and frequency-droop response.[187] NERC states that these capabilities will provide "significant" reliability benefits as DER deployments expand nationwide and flow increasing power to the BPS.[188]

IEEE 2800-2022 requires similarly advanced capabilities for BPS-connected IBRs. The standard includes performance requirements for voltage and frequency ride-through, active power control, reactive power control, dynamic active power support under abnormal frequency conditions, dynamic voltage support under abnormal voltage conditions, power quality, negative sequence current injection, and system protection—again, all critical for maintaining the reliability of an IBR-heavy grid.[189]

Enemy Exploitation

Many currently deployed inverters are replete with vulnerabilities, including those installed by non-utility purchasers. NIST assessed the latter category of inverters against its cybersecurity guidelines for such devices and found dozens of vulnerabilities across multiple commonly deployed products, including security flaws it deemed "critical."[190]

The risks created by these vulnerabilities will grow as inverters acquire additional grid-support features that adversaries will seek to misoperate. NERC, DOE, and their partners have identified "malicious control" of both BPS and DER IBRs through the internet as one of many new threat vectors that advanced IBR capabilities will enable, along with "misconfiguration of IBR/DER grid-support functions" that would lead to "dangerous conditions" and the "shutdown of IBR/DER networks."[191]

[184] This attribute of conventional generators is termed *inertial control*. Appendix A discusses inertial control, primary frequency response, and other frequency and voltage response mechanisms, as well as the broader set of ERSs the IBRs must help provide.

[185] Tarafdar Hagh et al., "Flexible Alternating Current Transmission System (FACTS)."

[186] On the ability of BESS to provide these reliability services, see DOE, *Battery Energy Storage Systems*,18–19.

[187] IEEE, IEEE 1547-2018; and NERC, *Perspectives on the Adoption of IEEE 1547-2018*, x–xv.

[188] NERC, *Perspectives on the Adoption of IEEE 1547-2018*, 23, 26, 28–31.

[189] IEEE, IEEE 2800-2022.

[190] McCarthy et al., *Cybersecurity for Smart Inverters*, Appendix F, 37–44.

[191] Johnson, Krishnappa, and Goodlett, *Solar Energy Cybersecurity*, 1.

The ride-through capabilities required by IEEE 1547-2018 constitute one such risk. DOE cautions that adversaries may seek to leverage those capabilities to "create instability in the grid by intentionally causing DER to disconnect from the grid during events when they should remain connected."[192] DOE warns that attackers could compromise DER firmware settings through communications networks belonging to the aggregator, the utility, or the DER vendor. Adversaries may also insert malicious firmware via a compromised DER vendor or aggregator.

Using such access, they could seek to alter DER over- or underfrequency settings. Once the DER settings are changed, "the attacker simply waits for a grid disturbance (fault or loss of generation) to cause widespread DER tripping," or—rather than wait for such disturbances—they could manipulate DERs to instigate tripping.[193] DOE warns that adversaries may also access DERs to misconfigure their settings. IEEE 1547-2018 provides default values for many functional settings for DER performance during normal and abnormal voltage and frequency conditions. However, the standard also requires that utilities and DSOs be able to modify those default values to account for site-specific and regional factors affecting grid operations.[194]

The adjustability of DER settings creates additional LotL attack vectors. For example, IEEE-compliant DERs can actively regulate grid voltage and provide frequency response.[195] IEEE 2800-2022 requires similar functionality for BPS-connected IBRs.[196] These capabilities can help limit the impact of grid disturbances. However, an adversary's misoperation of IBR frequency and voltage control capabilities at scale could create the very instabilities they are intended to limit. Put another way: the same advanced inverter capabilities that are essential to help protect the grid's reliability may threaten its security.

Inverter vendors' software and firmware updates magnify these dangers. Sungrow, a major Chinese provider of inverters to the US market, advertises that its new iSolarCloud "allows installers' accounts to do remote firmware upgrades at a click of a button" and "access all settings for the inverter remotely."[197] SolarFix boasts that its regular firmware updates improve safety features to prevent damage from faults or overloads and "avoid malfunctions that could cause serious and costly damage to your system."[198] Other major IBR vendors offer similar update services, including Ningbo Deye, SolarEdge, and other manufacturers of inverters for both utility-scale plants and smaller IBRs.[199]

In the wrong hands, these update capabilities could offer a devastating attack vector. The ability to "improve" IBR safety features and introduce (rather than mitigate) risks of equipment damage would be attractive as well. Moreover, adversaries could seek to exploit cloud-based firmware and software updates, centralized patching, and other operations to simultaneously introduce failure modes into vast numbers of inverters and other power electronics systems.

It is impractical to address these cyber risks by keeping inverters and other DER/IBR power electronics stupid. As such resources increasingly replace conventional generators and the ERSs they provide, solar, wind, and battery energy storage system assets must help replicate those services. The best way to manage the resulting cyber risks: ensure that as devices become increasingly smart, they are designed, manufactured, networked, and

[192] DOE, *Cybersecurity Considerations*, 23.

[193] DOE, *Cybersecurity Considerations*, 23.

[194] NERC, *Perspectives on the Adoption of IEEE 1547-2018*, xv.

[195] IEEE 1547-2018 also specifies that DERs may provide inertial response—that is, the capability to modulate active power in proportion to the rate of change of frequency (Narang, "Highlights of IEEE Standard 1547-2018," 24, 28).

[196] IEEE, IEEE 2800-2022.

[197] Sungrow, "Remote Firmware Upgrades," 1.

[198] SolarFix, "Role of Firmware Updates."

[199] Ningbo Deye, "New Firmware Version."

operated in ways that limit adversary opportunities to access and employ them for cyberattacks.

Secure-by-design principles can help manufacturers counter "Living off the Land" threats to grid components that are essential to ensure the reliability of an IBR-heavy grid.

Making DERs and IBRs Secure by Design—and in Depth

CISA's Secure by Design initiative establishes principles that can help manufacturers counter LotL threats to advanced inverters, updated equipment protection systems, and other grid components that are essential to ensure the reliability of an IBR-heavy grid.[200] As part of that initiative, CISA calls on software manufacturers to provide products that are "secure by default"—that is, installed with secure configurations that protect them against LotL attacks and other prevalent threats.[201]

DOE's *National Cyber-Informed Engineering (CIE) Strategy* offers recommendations to implement CISA's principles in the energy sector and beyond. DOE urges manufacturers to apply CIE strategies "first and foremost to the critical functions where cyber manipulation could result in unacceptable consequences"[202] (e.g., the simultaneous misoperation of IBRs and their control systems across the United States). The strategy also calls for the adoption of a defense-in-depth strategy that assumes that adversaries will compromise device protections and reduces the risk that a single failure will impact critical functions. Together with initiatives led by device manufacturers, these CISA and DOE recommendations provide the basis to prioritize and build in layered defenses for key grid components and control systems.

Communications Security

If adversaries can't communicate with inverters, they can't reconfigure and misoperate them. The CIE strategy calls for creating a secure information architecture by designing information pathways to ensure that data flows only in desired ways and that proper architectural controls enforce those information flows.[203]

Ensuring communications security for DERs will be complicated by the nature of the networks they employ. NERC notes that many of these resources are connected to the internet, and that their digitalization and associated connectivity requirements are continuing to expand "exponentially."[204] That internet connectivity can enable adversaries to access critical devices and infrastructure operations.[205] National Cyber Director Harry Coker Jr. warns that "the internet was not built on a secure platform. It was built for convenience, and security has not evolved at the pace and scale that it needs to."[206] The complex networks necessary to manage highly distributed resources provide adversaries with additional attack vectors. DOE states that DERs "will be managed in a different manner from traditional power operations due to their dispersed nature," including a reliance on internet-based remote control and monitoring.[207]

[200] Appendix C provides a detailed analysis of secure-by-design principles and their application to protection systems and other grid components.

[201] CISA et al., *Security-by-Design and -Default*, 5–6.

[202] DOE, *National Cyber-Informed Engineering Strategy*, 13. On implementing the strategy, see Gellner et al., *Critical Function Assurance*. On defense in depth, see also ICS-CERT, *Recommended Practice*, iii.

[203] DOE, *National Cyber-Informed Engineering Strategy*, 12.

[204] NERC, *Cyber Security for Distributed Energy Resources*, 1.

[205] Adversary hijacking of the internet's Border Gateway Protocol (BGP) offers an especially significant threat (Easterly and Rosenworcel, "Most Important Part of the Internet").

[206] Rundle, "White House Takes Aim."

[207] DOE, *Cybersecurity Considerations*, 8.

Government and industry have developed guidelines to help prevent attackers from accessing inverters via the internet and other communications networks. Among the most prominent:

- IEEE 1547.3-2023, *Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*, offers recommendations for cybersecurity practices and controls to ensure secure communication of DER protocols (e.g., IEEE 1815, IEEE 2030.5, SunSpec Modbus, and IEC 61850) specified in IEEE 1547-2018.[208] The guidelines include network engineering, access control, and data security measures.
- Industry-developed standards, including UL 2941, *Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources*, and the International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443 series of standards. These standards, respectively, (1) recommend testing requirements and protocols for application to DERs, and (2) define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems.[209]
- NIST's *Cybersecurity for Smart Inverters* guidelines and NARUC's *Cybersecurity Baselines Draft Informative References* include extensive recommendations on designing and implementing DER network security measures, including through the adoption of multifactor authentication techniques, cryptography, and zero-trust communications protocols.[210]

Schneider Electric, Northern Electric Power, and dozens of other US and allied inverter manufacturers are building security into their products to comply with (and in some cases, go beyond) UL 2941, ISA/IEC 62443, and government recommendations.[211] Gateways offer an especially important tool for communications security. Gateways connect communication networks that use different languages and translate those languages so that devices on one network can talk with devices on other networks, including multiple DER devices' utility, vendor, or aggregator networks that are managing the system. The Electric Power Research Institute and other organizations are partnering with manufacturers to refine and deploy gateways that securely connect these networks.[212] In addition, DOE is funding an array of research initiatives to strengthen communications protocols, encryption, and zero-trust technologies.[213]

DER network defenses face intensifying threats. YubiKeys exemplify the difficulties of doing so. YubiKeys are hardware tokens used by many DSOs for two-factor authentication. In September 2024, researchers identified a cryptographic flaw in these devices that makes them vulnerable to cloning attacks.[214] Closing additional defensive gaps, such as backdoor access opportunities via unsecured customer links to DERs, will require sustained innovation.

Yet, the most significant problems for DER communications security lie not in the adequacy of security guidelines or manufacturer technologies to comply with them, but rather with state adoption of measures to enforce the deployment of secure devices and communications protocols. As noted above, many states have yet to require compliance with IEEE 1547-2018 (setting DER performance

[208] IEEE, IEEE 1547.3-2023. For a comprehensive review of IEEE standards and other industry guidelines for IBRs, see Lyu and Xie, *Inverter-Based Resource Interconnection Standards*.

[209] UL, UL 2941; and ISA, "ISA/IEC 62443 Series of Standards."

[210] McCarthy et al., *Cybersecurity for Smart Inverters*; and NARUC, *Draft Informative References*.

[211] Schneider Electric, "Secure Development Lifecycle Process."

[212] Matz, "Network Gateway."

[213] DOE, "Selected Projects."

[214] Goodin, "YubiKeys Are Vulnerable."

standards) as a prerequisite for the approval of interconnection agreements. The establishment of state requirements for compliance with its cybersecurity counterpart, IEEE 1547.3-2023, lags far behind those efforts. A California Public Utilities Commission working group has begun considering new communications security rules based on IEEE 1547.3-2023.[215] Other state PUCs should follow suit, given the accelerating deployment of smart inverters that adversaries can exploit.

Applying these recommendations to aggregators and other commercial DER companies poses additional challenges. NERC notes that they do not typically use IEEE 1547-2018-specified interfaces, but instead employ a variety of other interfaces for which there are currently no security requirements at all. Moreover, public internet access for DERs utilizes Wi-Fi and cellular 4G/5G wireless networks, which are susceptible to interception and require strong encryption and authentication. Wired Ethernet and fiber-optic networks can be compromised through physical access or device vulnerabilities at the site of the DER endpoint. And regardless of the medium for access, the use of public internet leaves both DER and DER aggregator control systems exposed to remote attacks from anywhere on the globe.[216]

Constraints on Device Functionality

As we intensify efforts to protect DER communications systems, we should also assume that those defenses may fail and we should therefore make inverters secure by default so they cannot be misoperated even if adversaries gain access to them. Secure-by-default products "are resilient against prevalent exploitation techniques out of the box without additional charge. These products protect against the most prevalent threats and vulnerabilities without end-users having to take additional steps to secure them." Most important, "a secure configuration should be the default baseline" to "automatically enable the most important security controls needed to protect enterprises from malicious cyber actors, as well as provide the ability to use and further configure security controls at no additional cost."[217]

UL 2941 and NIST's guidelines encourage manufacturers to continue designing cybersecurity into DERs.[218] Some of these measures have already been widely adopted. For example, NIST recommends that "smart inverters should control the interactions among different functions and services within the device. This includes physical or software protection of real-time control functions and power electronics from data communications interfaces." To protect against unauthorized or malicious software updates, smart inverters also should have a list of known trusted sources from which they will accept software updates and should authenticate those sources.[219] Many US and allied manufacturers sell devices with these features.

In addition, as inverters gain more sophisticated capabilities, manufacturers should adopt stretch goals to apply secure-by-design/default principles. One option: assess whether and how firmware could constrain inverter capabilities so that these devices have sufficient frequency and voltage control functions to help limit grid disturbances (and also enable utilities to adjust their configurations to meet local needs), but not so much functionality that adversaries could misoperate them to create instabilities or outages.

IBR providers, regulators, and grid operators should also apply lessons learned from other sectors to bolster their own device-level security efforts. The Protecting and Transforming Cyber Health Care Act of 2022 (PATCH Act) provides one such model.

[215] CPUC, *Working Group Report*.

[216] NERC, *Privacy and Security Impacts*, 10–11.

[217] CISA et al., *Security-by-Design and -Default*, 5–6.

[218] UL Solutions, "Cybersecurity Certification."

[219] McCarthy et al., *Cybersecurity for Smart Inverters*, 16–17.

The act provides for a holistic life-cycle approach to secure medical devices from cyberattacks. To help implement the PATCH Act, the Food and Drug Administration issued recommendations on the security features that such devices should include when manufacturers request approval to market them.[220] The life-cycle security requirements embedded in these initiatives could be especially valuable to apply to the electric system.

Device Installation and Configuration

Even if manufacturers build security into inverters, IBR operators' failure to properly deploy those devices can still create risks to reliability and system security. NERC found in November 2023 that despite its repeated issuance of alerts and voluntary guidelines on IBR performance, these recommendations "are not being implemented" by BPS operators.[221] Implementation of future performance standards at the distribution level will be still more problematic. For aggregators and other new entrants who have little experience with standards compliance and far less technical expertise than BPS utilities, ensuring the effective implementation of such standards (and the secure integration of DER system components) will present major challenges.

DOE should expand its current assistance programs to help aggregators meet these implementation requirements. As part of the Bipartisan Infrastructure Law, the Grid Deployment Office is administering a $10.5-billion Grid Resilience and Innovation Partnerships (GRIP) Program to enhance grid resilience. The program's Digital Assurance technical assistance track provides an ideal means to help aggregators, VPPs, and small distribution utilities met the challenge of standards implementation and secure system integration.[222]

Employing Energy Management Systems for Defense

If adversaries gain access to inverters by evading their device-level protections, an additional layer of defense could still help protect the grid: security measures embedded in distributed energy resource management systems (DERMS).

DERMS and other mass orchestration platforms serve as central management systems that enable the coordination of large numbers of dispersed generation and storage resources and provide real-time monitoring, control, and coordination functions to maintain grid stability.[223] PRC exploitation of these centralized control functions could create catastrophic effects. DOE warns that if adversaries infiltrate the control systems applications of such a system, they could manipulate its wide-area control requests and issue corrupted commands, "causing power system instability or power losses" and "potentially compromising its entire DER fleet."[224]

DOE and industry should flip the script and build new capabilities into DERMS to limit the effects of cyberattacks conducted at scale by misoperated inverters and other devices. In contrast to the PRC's dominance of inverter and BESS manufacturing, the market leaders for DERMS include GE Vernova, Siemens, Schneider Electric, ABB, and other US/allied companies.[225] DOE and industry should leverage this comparative advantage to build secure-by-design features into DERMS platforms to prevent their misoperation. These partners should also explore how AI-enabled DERMS control software could help defend distribution systems from adversary-induced frequency and voltage instabilities. Ideally, as DER and IBR deployments grow across the United States, utilities and reliability coordinators will be able to integrate

[220] PATCH Act; and FDA, *Cybersecurity in Medical Devices*.

[221] NERC, *Inverter-Based Resource Performance Issues Report*, iv.

[222] DOE, "GRIP Program."

[223] DOE, *Battery Energy Storage Systems*, 34.

[224] DOE, *Cybersecurity Considerations*, 27.

[225] DOE, *Battery Energy Storage Systems*, 60–61.

these advanced DERMS capabilities into their broader plans for cyber incident response.

While operators gain additional opportunities for load management, adversaries will gain new attack opportunities as well.

Countering Demand-Side Attacks

During severe weather events and other emergencies that create imbalances between the supply and demand for power, grid operators can ask customers to limit their power consumption or—in extremis—conduct rolling blackouts or other drastic measures to protect grid reliability.[226] The growth of BESS and massive new controllable loads, including EVs and their charging stations, cryptocurrency mining facilities, and other large-scale electricity customers, will give these operators additional opportunities for load management.

Adversaries will gain new attack opportunities as well. Attackers can seek to cause drastic changes in system loads to create instabilities and disruptive power swings, and—especially in conjunction with the disruption of protection systems and power supplies—cause blackouts and equipment damage.[227] Countering these threats will entail new requirements for grid resilience strategies and further widen the range of industries, regulators, and government authorities that will need to collaborate across their jurisdictional divides.

Electric Vehicles and Charging Stations

The Trump administration has taken a number of actions that will slow the growth of EV sales and the deployment of charging stations, including orders to halt distribution of unspent federal funds for such stations.[228] Nevertheless, EVs could soon offer a significant source of energy storage that could help grid operators conduct balancing operations and, potentially, provide frequency and voltage support to limit the impact of grid disturbances. These vehicles were originally designed for one-way power flows; similar to cell phones, they would draw power from the electric grid as needed to keep them charged. However, with advances in EV power electronics, charging station capabilities, and other infrastructure and control systems, EVs are now capable of bidirectional flows of electricity with the grid. Especially useful, EVs can charge up during periods of low demand for electricity (typically at night) and then send power to the grid when demand is high. Moreover, with the help of smart inverters, such vehicle-to-grid operations can now support grid reliability and can be structured to provide the equivalent of mobile, distribution-level BESS.[229]

EV storage may soon offer additional benefits for grid management. DOE notes that with the utilization of smart inverters and other advanced power electronics, EV-provided energy storage can support voltage control and contribute to system frequency response.[230] All of these attributes could help grid operators not only to support day-to-day grid reliability as variable wind and solar generation grows but also to respond to instabilities caused by extreme weather events or adversary attacks.

[226] Appendix A provides additional details on load shedding and other load management tools for emergency response operations.

[227] Amini, Pasqualetti, and Mohsenian-Rad, "Dynamic Load Altering Attacks"; Mohan, Meskin, and Mehrjerdi, "Cyber-Attacks and Cyber Security"; and Johnson et al., "Power System Effects."

[228] Shepardson, "Trump Revokes Biden 50% EV Target."

[229] Choi, "Essential Grid-Scale Storage"; Mafazy, *Vehicle-to-Grid (V2G) Standards*, 4–5; and EAC, *Enhancing Grid Resilience*.

[230] EAC, *Enhancing Grid Resilience*, 3; and NERC, *Electric Vehicle Dynamic Charging Performance*, 8.

Employing EV batteries to support reliability will entail a host of unresolved problems. The most significant may be behavioral rather than technical. As one utility CEO has said, "when it looks like China is going to attack, I want my Tesla fully charged and ready to go, not drained off for some other use."[231] A partial solution may be to have large government or private-sector fleets (including those operated by utilities) under contract with BPS entities to provide power in emergencies.[232] But for the tens of millions of EVs operated by private citizens, behavioral factors will cast doubt on the availability of those resources to help manage cyber-induced instabilities.

EVs also create problems for reliability that the PRC may seek to exacerbate. A working group comprising EV organizations, NERC, and other grid reliability stakeholders found that the "effects of grid dynamics, controls, and system stability due to the power electronic behavior of the EV charging loads may create new risks of widespread, cascading blackouts." Their research also determined that when grid disturbances originate from the BPS, EV charging behavior could exacerbate the resulting disruptions to the electric system and may result in "catastrophic consequences for grid reliability if left unchecked."[233] Adversaries seeking to magnify the consequences of their attacks on the BPS could find these EV charging effects useful indeed, especially if they can directly target EV charging operations by accessing their internet-connected controls to create large-scale, disruptive shifts in power flows.

Government and private initiatives are now underway to develop technologies that can mitigate these threats. DOE is funding research and collaborating with the Department of Transportation (DOT) and the private sector to improve cybersecurity for secure EV charging.[234] To help guide such efforts, NIST issued a report titled *Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure*, which provides users with a national-level risk-based approach for managing cybersecurity activities.[235] The National Renewable Energy Laboratory and other national laboratories are also collaborating with industry on EV research.[236]

A more structured, federally led approach will be needed to develop and enforce cybersecurity standards for EVs and their charging infrastructure. NERC established the Electric Vehicle Task Force to collaborate with EV charging companies and other industry partners on interconnection requirements and other reliability-related issues.[237] The Bipartisan Infrastructure Law created the Joint Office of Energy and Transportation to facilitate collaboration between DOE and DOT to support the build-out of EV-related infrastructure.[238] DOD's Cyber Warfare's Risk to Mission Methodology program is also examining EV risks and mitigation options.[239] As these disparate efforts go forward, DOE should task its ESIB to guide collaborative efforts with DOT, other federal agencies, and industry to establish EV cybersecurity standards.

The ESIB is designed to support such integrative efforts. When DOE established the ESIB in February 2022, it stated that it would encompass "the energy sector and associated supply chains that include all industries, companies and stakeholders directly and indirectly involved in the energy sector."[240] EVs and their charging infrastructure

[231] Private communication with the author.

[232] T&D World, "EV Fleet Grid-Enhancing Pilot Program."

[233] NERC, *Electric Vehicle Dynamic Charging Performance*, 5, 1.

[234] DOE, "Securing EV Charging Infrastructure."

[235] McCarthy et al., *Cybersecurity Framework Profile*.

[236] NREL, "Cybersecurity for Electric Vehicle Grid Integration."

[237] NERC, *Electric Vehicle Task Force*.

[238] Joint Office of Energy and Transportation, "About."

[239] White House, *Energy Modernization Cybersecurity Implementation Plan*, 38.

[240] Igogo et al., *America's Strategy*, ix. Exec. Order 14017 on America's supply chains directed the secretary of energy to

depend on the energy sector and pose significant (and intensifying) threats of disrupting it. Since establishing the ESIB, however, DOE has done little to employ it for cybersecurity in ways that leverage its integrative, multi-industry potential.

The defense industrial base provides a model for such integration. It brings together myriad industries to coordinate against cyber threats to their defense products and support activities. The ESIB can do the same for the grid, deepening coordination between utilities and industries that pose potential threats to their operations. Collaborating with DOT, vehicle and charging station manufacturers, and other stakeholders in EV resilience offers an ideal use case for launching the cybersecurity work of the ESIB.

Yet, while EVs exemplify the multi-sector challenge of countering demand-side attacks, other threats both within the electric system and far beyond it require still more innovative approaches. Three such threats merit special attention: advanced metering infrastructure (AMI) systems, the IoT, and information operations (IOs).

Smart systems provide immense benefits for electricity customers and utilities alike. They also enable adversaries to conduct load manipulation attacks with unprecedented scale and precision.

Exploiting Advanced Metering Infrastructure

AMI systems provide immense benefits for electricity customers and utilities alike. Thanks to the internet connectivity of smart meters and their associated control systems, AMI can conduct bidirectional communications with other grid devices to allow remote meter readings, undertake maintenance functions, and control loads in ways that can save customers money. AMI also enables new forms of demand management. Most important, consumers can reduce or shift their electricity usage during peak periods in response to time-based rates or other financial incentives.

These same advanced capabilities and communications links will enable adversaries to conduct load manipulation attacks with unprecedented scale and precision. The most obvious threat vector: by simultaneously switching millions of smart-meter loads on and off repeatedly, adversaries can seek to disrupt balancing operations to destabilize the grid and create cascading outages.[241] Many other attack opportunities exist as well. Adversary options include the disruption of AMI communications protocols, denial or corruption of system data, issuance of remote disconnection commands, distributed denial-of-service attacks, and man-in-the-middle attacks.[242] In addition, researchers are identifying new vulnerabilities that reflect AMI software's increasing data management and control features, including the ability of adversaries to remotely install and run codes of their choice on smart meters.[243]

An additional risk factor: no mandatory cybersecurity standards exist for the AMI that is already installed across the United States and will remain in place for years to come. Existing voluntary guidelines could help secure future AMI deployments.[244] Standards also exist for some components of an AMI system, including for radio communications

submit a supply chain strategy overview report for the ESIB (as determined by the secretary of energy).

[241] Gurzu, "Hackers"; DOE, *Advanced Metering Infrastructure*, 69; and Hansen, Staggs, and Shenoi, "Security Analysis," 3.

[242] A detailed and comprehensive assessment of these attack opportunities is provided by Shokry et al., "Systematic Survey." See also Khattak, Khanji, and Khan, "Smart Meter Security."

[243] Seals, "Critical Security Hole."

[244] EPRI, *Risk Assessment and Security Requirements*.

covered by IEEE 802.15.4.[245] Compliance with voluntary international standards for certain AMI components can also help address their security challenges.[246] In addition, government and industry initiatives are underway to better understand the vulnerabilities of AMI components and develop protections against them.[247] Staying ahead of the threat and transitioning voluntary guidelines to enforceable standards should become a priority for regulators and their industry partners.

The Internet of Things

The growth of the IoT will magnify the danger of demand-side attacks. By 2025, the total number of consumer and industrial IoT connections in North America is forecast to grow to 5.4 billion.[248] Many of these devices constitute significant new loads the grid will have to manage either individually (as in the case of multi-megawatt data centers) or in aggregate. As an example of the latter category, "smart building" systems for HVAC systems are increasingly internet connected and create a massive demand for power. IoT devices offer great flexibility to system operators, such as participation in load relief programs or demand response programs. Enabling the quick control of air conditioners and other end-use devices could eventually help alleviate grid constraints or reliability issues, as could EVs and AMI-controlled loads.[249]

Again, however, this controllability entails threats to grid reliability and security. Malicious control of many thousands of IoT loads could have a serious impact on BPS reliability, particularly during stressed system conditions. For example, widespread manipulation of internet-connected heating and cooling systems, commercial drives, and other elements could rapidly alter energy consumption patterns at both distribution and transmission levels. Unexpected load consumption during severe weather events or near-instantaneous changes in load consumption could pose serious risks to the grid since existing protections and controls are not accustomed to handling these types of unexpected operations.[250]

The PRC is well positioned to conduct such attacks. Two Chinese companies, Quectel and Fibocom, dominate the global market for IoT cellular modules that connect smart devices with the internet. Chair Mike Gallagher and ranking member Raja Krishnamoorthi of the House Select Committee on the CCP note that these modules are used in a wide variety of devices across the United States, including in smart cities, EVs, and telecom networks. Given that the modules can brick such IoT components at scale, these legislators warn that such capabilities raise "particular grave concerns in the context of critical infrastructure."[251] From a grid perspective, such concerns include the danger of large-scale load manipulation to create system instabilities.

Gallagher and Krishnamoorthi have called on the FCC to address these dangers of IoT manipulation. Other efforts to secure IoT devices are already underway. Executive Order 14028 directs NIST to recommend requirements for a cybersecurity labeling program for consumer IoT products. NIST is now developing a set of foundational recommendations that provide a starting point for securing a

[245] Oxlee, "Cybersecurity Vital."

[246] For example, "radio communications is generally covered by IEEE 802.15.4 (the technical standard which defines the operation of low-rate wireless personal area networks)" (Oxlee, "Cybersecurity Vital").

[247] Especially significant: Congress has required DOE to provide a report on the cybersecurity of distribution systems, including on load management devices that help make up AMI (Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 40121).

[248] Petroc, "IoT Connections."

[249] Timberlake, "Hackers Target HVAC."

[250] Alcade et al., *Integrating Cyber and Physical Security*, 103.

[251] Gallagher and Krishnamoorthi, letter.

broad range of IoT devices.[252] Industry-led efforts are also seeking to help secure IoT devices. For example, IEEE 2413-2019, *Standard for an Architectural Framework for the Internet of Things (IoT)*, establishes a conceptual basis for assessing IoTs and provides a collection of perspectives on IoT architecture.[253] However, the process of establishing voluntary (much less mandatory) security standards for IoT devices is progressing much more slowly than the deployment of these highly controllable, and manipulable, loads. As with EVs, the ESIB might facilitate a multi-industry effort to develop such standards. But the United States should pursue whatever interagency options enable the quickest progress against IoT threats to the grid.

Information Operations to Enhance Demand-Side Attacks

With the growing frequency and severity of extreme weather events, utilities are increasing their use of customer messaging to support demand-side emergency operations. During a 2022 heat wave in the Southwest, for example, "millions of Californians' cellphones lit up with a new type of emergency alert: 'Conserve energy now to protect public health and safety.'" That message quickly changed customer behavior and power consumption. Elliot Mainzer, president and CEO of the California Independent System Operator (which manages the flow of electricity on high-voltage power lines), stated that "within moments, we saw a significant amount of load reduction . . . of approximately 2,000 megawatts over the next 20 to 30 minutes." He also noted that this "response from California consumers to the wireless emergency alert allowed us to restore our operating reserves and took us back from the edge of broader grid disturbance."[254]

Utilities are also employing customer messaging to manage severe cold weather events. In the December 2022 "bomb cyclone" that brought historic freezing temperatures to Pennsylvania and neighboring states served by PJM, the area's regional transmission organization (which also manages high-voltage power flows), cold weather knocked out as much as forty-six thousand megawatts of generation capacity that either would not start when PJM called on it or tripped offline while it was running.[255] PJM helped manage the consequences of this loss by successfully urging millions of customers in the region to reduce their demand for power.[256] Furthermore, grid operators already have extensive expertise in accounting for human behavior-driven variations in load. For example, during NFL Super Bowls, energy usage spikes during halftime and commercial breaks as viewers use microwaves and other electric-powered devices.[257]

We are now entering an era of contested information environments. China and Russia have been waging disinformation campaigns against the United State for years to influence elections, corrode US citizens' faith in democratic governance, and achieve other strategic goals. In a severe crisis over Taiwan or other regional flashpoints, adversaries could pair IOs with cyberattacks to incite public panic and magnify the effectiveness of their operations against the US homeland. Grid managers increasingly use social media and cell messages to shape customer behavior in ways that support grid reliability. Now, we must prepare for adversary efforts to shape behavior in disruptive ways, especially as deepfakes, voice fakes, and other advances in technology increase the potential effectiveness of such IOs.

A recent Chinese-edited journal article explores how adversaries can send fake discount notifications

[252] Fagan et al., *IoT Core Baseline*.

[253] IEEE, IEEE 2413-2019.

[254] Toohey and Petri, "Text Asked Millions of Californians."

[255] PJM, *Winter Storm Elliott*, 49.

[256] PJM, *Winter Storm Elliot*, 120–124; and Behr, "Bomb Cyclone."

[257] University of Tennessee, "Superbowl Frequency Swings."

to customers to encourage them to recharge their EVs during peak demand periods. Using Greater London as a case study, the article describes how IOs might indeed lead unwitting consumers to synchronize their energy usage patterns, resulting in city-scale blackouts if the grid is heavily loaded.[258]

Of course, adversaries do not need to rely on IOs alone to create stability problems for the grid. They may combine IOs with cyberattacks to manipulate both the demand and supply of power, thereby seeking to maximize power swings and grid instabilities. The PRC created the Strategic Support Force in 2025 to integrate cyber, IOs, space, and electronic warfare into the PLA's integrated joint operational warfighting structures. China announced in April 2024 that it was dissolving the Strategic Support Force and establishing separate commands for an Aerospace Force, Cyberspace Force, and Information Support Force (ISF). Xi Jinping assigned the ISF with "a great responsibility for advancing the military's high level of development and winning a modern war."[259] Pairing ISF psychological operations efforts with cyberattacks against the grid would be especially well suited to help the PRC achieve its goals of inducing societal panic and impeding US decision-making. As the Trump Administration reassesses (and in significant respects, downsizes) broader federal efforts to counter disinformation, preparedness against combined Chinese cyber–information attacks should be treated as a special case and elevated as grid resilience priority.

Conclusion and Summary of Appendixes

The United States has a historic opportunity to strengthen the electric system's resilience against PRC attack, but only if we seize it. In addition to continuing decades-old approaches to cybersecurity, especially by supplementing NERC standards to protect IBRs, the United States should also adopt an entirely new defensive strategy that capitalizes on grid decentralization.

Indeed, we must take that new path. Given the explosive growth of DERs, their unprecedented importance to the electric system, and their myriad vulnerabilities to PRC exploitation, it is no longer sufficient to rely on voluntary guidelines to secure these systems. PUCs and their public power and rural cooperative counterparts should partner with government leaders to establish mandatory, risk-based standards for DERs, and they should do so before a catastrophic attack impels their adoption. In addition, given the dangers of demand-side attacks that manipulate the IoT and other massive loads, DOE should build collaboration across the broader array of government and private-sector stakeholders that are now crucial for grid resilience.

It is tempting, however, to focus only on security problems of decentralization and overlook its potential upside. That is understandable: as noted in the beginning of this report, security goals played almost no role in driving the growth of DERs, which were instead spurred by decarbonization policies and related financial and market inducements. These policies may soon change at the federal level (though California, New York, and other states will likely seek to maintain their own carbon reduction targets). Nevertheless, with the millions of DERs that are currently installed and the nationwide, utility-scale IBRs that are connected to the BPS or are under construction, the United States already has the foundation it needs to adopt a new strategy for grid resilience and shape future deployments of IBR/DERs, SMRs, and other dispersed resources and control systems to help implement it.

This report proposes specific components of such a strategy and how they can help counter the goals that Chinese leaders will seek to achieve in attacking the grid. Some of these initiatives, such as the

[258] Raman et al., "Weaponizing Disinformation."

[259] Bruzzese and Singer, "Farewell to China's Strategic Support Force."

build-out of microgrids and plans for larger power islands to support force projection and protect society, are within easy reach. Others, such as the use of widely dispersed GFM resources rather than centralized cranking paths to help protect power restoration from PRC disruption, will require significant technical, modeling, and operational advances. The ultimate focus of all such efforts: strengthen the grid's resilience so effectively that the benefits Xi Jinping hopes to achieve by attacking it are dwarfed by the costs he expects to incur, and thereby help reduce the likelihood that such attacks will ever occur.

Summary of Appendixes

The grid's transformation and PRC attack capabilities create threats to resilience beyond those analyzed thus far in the report. Three appendixes (included in only the online report[260]) examine these threats and options to mitigate them, in the context of (1) skyrocketing requirements for power, including from AI data centers on which the US economy and national defense increasingly depend; and (2) new technological and computational capabilities to bolster grid reliability and resilience, ranging from the use of advanced inverter and EV battery capabilities to AI-supported control of future grid operations. The findings and recommendations of these appendixes are summarized below.

Appendix A Resource Adequacy, Cyber Contingency Response, and Power Restoration in an Inverter-Heavy Grid

Decentralizing and hardening the grid will offer little benefit if we don't have enough power to serve US customers. Two forces are squeezing the electric system in a vice grip. On the demand side, AI data centers, crypto manufacturing, and electrification of manufacturing and many other economic sectors are increasing electricity consumption far beyond the levels that shaped previous grid investment plans. On the supply side, deployments of DERs/IBRs are growing more slowly than many grid managers had hoped, while retirements of older gas-fired generators are accelerating faster than expected. The net result, according to NERC: "most of the North American BPS faces mounting resource adequacy challenges" and intensifying risks to system reliability.[261]

For defense against PRC attacks, this vice grip creates dangers for cyber response operations. The most urgent risk is the lack of sufficient operating reserves to prevent the spread of cyber-induced instabilities. NERC requires balancing authorities to maintain reserves of generation capacity at all times to help mitigate the effects of unexpected contingencies. However, NERC's reserve requirements are totally inadequate to respond to wide-area PRC-induced disruptions.

Shortfalls in resource adequacy are also creating problems for powering the AI data centers that are crucial for national security. DOD increasingly relies on AI services provided by data centers to plan for and execute regional wars, including those in the Taiwan Strait and elsewhere in the Far East. As construction of these data centers accelerates across additional US regions, deploying generation resources of all types that are colocated with those facilities will expand the broader benefits of grid decentralization.

Yet, advanced IBRs and DERs can also help counter PRC attacks in unique ways. This report briefly reviews opportunities to strengthen the resilience of US power restoration infrastructure and operations by employing dispersed GFM batteries. The analysis that follows explores these options in greater detail. The appendix also takes a deeper look at opportunities to employ EV batteries to limit the disruptive effects of cyberattacks.

[260] Available at https://www.jhuapl.edu/sites/default/files/2025-3/SurfingTheWave-WEB.pdf.

[261] NERC, *2024 Long-Term Reliability Assessment*, 6–7.

As is true of other aspects of IBR/DER deployments, however, their expansion also creates novel (and in some cases, poorly understood) attack vectors. The report examines how the PRC can seek to access and misuse advanced inverter capabilities for frequency and voltage control. The appendix recommends further analysis of an additional, especially high-consequence risk: the danger that deeper IBR penetrations will jeopardize the effectiveness of grid protection systems and help the PRC damage or destroy transformers and other critical grid equipment.

Appendix B Employing (and Securing) Artificial Intelligence for Grid Resilience

Advances in Chinese AI capabilities could jeopardize the security benefits of grid decentralization.[262] The nationwide dispersal of inverter-based generation, storage, and control systems will offer few advantages if China can use AI to precisely map these assets and simultaneously attack them. The solution: expand our own use of AI to defeat such attacks and turn the grid's increasing automation to our advantage.

AI already plays crucial roles in decentralized grid operations. DOE emphasizes that with the deployment of millions of DERs across the electric system and the need to coordinate complex, two-way power flows between distribution systems and the BPS, AI is now an "essential tool" to facilitate this coordination.[263]

Dependence on AI to support human decision-making is especially heavy for aggregators, VPPs, and smaller DSOs that lack the staffs of traditional utilities. These DER operators employ AI-enhanced DERMS, automatic distribution management systems, and integrated sensor networks to help them perform functions that once required large, highly trained staffs. The cost savings and operational efficiencies provided by AI tools are also spurring their adoption by larger distribution utilities and BPS entities.

The PRC is likely monitoring our use of AI for decision support and devising ways to exploit it. Utilities and regulators should ensure that for critical support functions, they employ only AI applications that meet security measures proposed by NIST and other sources of guidance. Compliance with those measures will be crucial as well for AI tools help utilities detect, assess, and respond to cyber intrusions.

Advances in AI defensive capabilities are creating a further issue: determining whether and how much to replace people with machines. Cybersecurity employees in BPS control rooms have long believed that humans should be in, or at least over, the loop of defense operations. Cybersecurity teams in many BPS entities already use AI for decision support against cyberthreats. With the imperative for split-second mitigation actions, and increasingly capable AI tools, the shift from support to lead is already underway.

There is no single answer to how far that transition should go. Utilities need to assess the comparative advantages of humans and AI for specific defense functions and invest in both AI and human-led capabilities necessary to defeat machine-speed attacks.

Appendix C Forging Unity of Effort Across the US Electric System

Implementing the transition from voluntary to mandatory DER cybersecurity standards is vital

[262] As used in this study, the term *artificial intelligence*, or AI, has the meaning set forth in 15 U.S.C. 9401(3): "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action." This definition is also used in Exec. Order 14110.

[263] Benes, Porterfield, and Yang, *AI for Energy*, 20–21.

but fraught with difficulties. The main report offers proposals to facilitate that shift, starting with the establishment of a nationwide registry of aggregators and VPPs so that distribution utilities can apply security requirements to their interconnection agreements. This appendix examines three additional steps to help transform voluntary measures into mandatory ones on a prioritized, risk-informed basis.

The first is establishing a new regulatory construct to assess reliability and cyber resilience investments and enable cost recovery for them. Distribution-level regulators and utilities focus on assessing and improving the ability of individual distribution systems to provide reliable service to their customers, as measured by the customer Average Interruption Duration Index (CAIDI), the Customer Average Interruption Frequency Index (CAIFI), and related metrics. These metrics remain useful. However, their focus on individual utilities reflects a bygone threat era. Regulators and other authorities for distribution systems should supplement them to account for the systemic threats to US power distribution nationwide and apply those metrics to assess the prudence and costs avoided by investments in resilience.

A second imperative to secure the DER-heavy grid lies in creating shared standards, versus having fifty-four states and territories develop their own requirements. The Electricity Subsector Coordinating Council is ideally suited to collaborate with the trade associations for local distribution systems, rural cooperatives, and public power utilities to prioritize and develop consistent security mandates.

The third challenge to implementation is cost. The expense of securing the decentralized grid, versus leaving it vulnerable to catastrophic failures, depends on a vast number of variables. But GFM inverters provide a promising data point. Inverters capable of blackstart restoration and frequency and voltage control for cyber incident management are only 2 to 5 percent more expensive than their grid-following (GFL) counterparts. At a time of climbing electricity prices, even modest security-driven increases will be of concern to ratepayers.

Adopting a new rule of thumb can help limit ratepayer bills. If projects directly (and primarily) protect the flow of power to specific defense installations or other facilities critical for national security, the federal government should fund those investments. If projects improve the reliability of service to all utility ratepayers in a given service area, the costs of those investments should be borne more broadly via tariffs, rate cases, and other established means of cost recovery.

Bibliography

Accelerate Group and EPIC (Electric Program Investment Charge) Policy + Innovation Coordination Group. *Transportation Electrification Workstream Report*. Sacramento, CA: California Energy Commission, February 2021. https://www.epicpartnership.org/resources/Transportation_Electrification_Workstream_Report_Final.pdf.

Acharya, Samrat, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective." *IEEE Access* 8 (2020): 214434–214453. https://doi.org/10.1109/ACCESS.2020.3041074.

Alcade, Richard, Sam Chanoski, Johnny Gest, Jessica Harris, Mohammad Reza Khalghani, Roger Hales, David Sopata, and John Stewart. *Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector (TR105)*. Technical Report PES-TR105. New York: IEEE, December 2022. https://resourcecenter.ieee-pes.org/publications/technical-reports/PES_TP_TR105_PSCC_120622.html.

Amini, Sajjad, Fabio Pasqualetti, and Hamed Mohsenian-Rad. "Dynamic Load Altering Attacks against Power System Stability: Attack Models and Protection Schemes." *IEEE Transactions on Smart Grid* 9, no. 4 (2018): 2862–2872. https://doi.org/10.1109/TSG.2016.2622686.

ANL (Argonne National Laboratory). *Glossary*. Solar Energy Development Programmatic EIS (Solar PEIS). https://solareis.anl.gov/glossacro/dsp_wordpopup.cfm?word_id=4592.

ANSI EVSP (American National Standards Institute Electric Vehicles Standards Panel). *Roadmap of Standards and Codes for Electric Vehicles at Scale*. Washington, DC: ANSI, June 2023. https://share.ansi.org/evsp/ANSI_EVSP_Roadmap_June_2023.pdf.

Antonio, Katherine, and Alex Mey. "U.S. Battery Storage Capacity Expected to Nearly Double in 2024." *In-Brief Analysis*, January 9, 2024. https://www.eia.gov/todayinenergy/detail.php?id=61202.

APPA (American Public Power Association). "Our Members." https://www.publicpower.org/our-members.

———. *What Is Public Power?* https://www.publicpower.org/system/files/documents/municipalization-what_is_public_power.pdf.

Aschenbrenner, Leopold. "Situational Awareness: The Decade Ahead." *For Our Posterity* (blog), June 14, 2024. https://situational-awareness.ai/wp-content/uploads/2024/06/situationalawareness.pdf?ref=forourposterity.com.

Aurora Energy Research. "Aurora Report Finds Northern Virginia Data Center Demand Could Incentivize up to 15 GW of Additional Natural Gas Generation by 2030." June 20, 2024. https://auroraer.com/media/new-aurora-report-finds-northern-virginia-data-center-demand-could-incentivize-up-to-15-gw-of-additional-natural-gas-generators-by-2030/.

AWS Public Sector Blog Team. "AWS Announces AWS Modular Data Center for U.S. Department of Defense Joint Warfighting Cloud Capability." *AWS Public Sector Blog*, February 23, 2023. https://aws.amazon.com/blogs/publicsector/announcing-aws-modular-data-center-u-s-department-defense-joint-warfighting-cloud-capability/.

Barnes, Joe. "Bases Plagued by Mystery Drones Chose Not to Shoot Them Down, Pentagon Reveals." *Yahoo News*, October 16, 2024. https://www.yahoo.com/news/bases-plagued-mystery-drones-chose-174247844.html.

Bartz, Diane, and Alexandra Alper. "U.S. Bans New Huawei, ZTE Equipment Sales, Citing National Security Risk." Reuters, November 30, 2022. https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/.

Basrai, Huzaifah. "Accelerating Utility Rate Case Filings with Generative AI." *Utility Dive*, October 22, 2024. https://www.utilitydive.com/news/accelerating-utility-rate-case-filings-generative-ai-artificial-intelligence-genai/730551/.

Behr, Peter. "Bomb Cyclone Sparks Fierce Debate over Grid Readiness." *E&E News*, January 3, 2023. https://www.eenews.net/articles/bomb-cyclone-sparks-fierce-debate-over-grid-readiness/.

———. "EVs: The Next Grid Battery for Renewables?" *E&E News*, March 30, 2022. https://www.eenews.net/articles/evs-the-next-grid-battery-for-renewables/.

———. "Wanted: "Superhuman' AI to Master a Greener Grid." *E&E News*, August 23, 2021. https://www.eenews.net/articles/wanted-superhuman-ai-to-master-a-greener-grid/.

Bell, John. "Army Boosts Installation Resilience, Combat Readiness by Investing in New Energy Technologies." US Army, March 28, 2023. https://www.army.mil/article/265218/army_boosts_installation_resilience_combat_readiness_by_investing_in_new_energy_technologies.

Benes, Keith J., Joshua E. Porterfield, and Charles Yang. *AI for Energy: Opportunities for a Modern Grid and Clean Energy Economy*. Washington, DC: US Department of Energy, April 2024. https://www.energy.gov/sites/default/files/2024-04/AI%20EO%20Report%20Section%205.2g%28i%29_043024.pdf.

Bieler, Stephanie, Cara Goldenberg, Avery McEvoy, Katerina Stephan, Alex Walmsley, et al. *Aggregated Distributed Energy Resources in 2024: The Fundamentals*. Washington, DC: National Association of Regulatory Utility Commissioners, July 2024. https://connectedcommunities.lbl.gov/sites/default/files/2024-07/NARUC_ADER_Fundamentals_Interactive.pdf.

Blair, Nate, Chad Augustine, Wesley Cole, Paul Denholm, Will Frazier, Madeline Geocaris, Jennie Jorgenson, Kevin McCabe, Kara Podkaminer, Ashreeta Prasanna, and Ben Sigrin. *Storage Futures Study: Key Learnings for the Coming Decades*. NREL/TP-7A40-81779. Golden, CO: National Renewable Energy Laboratory, 2022. https://www.nrel.gov/docs/fy22osti/81779.pdf.

Blankenship, Doug, Charles Gertler, Mohamed Kamaludeen, and Michael O'Connor. *Pathways to Commercial Liftoff: Next-Generation Geothermal Power*. Washington, DC: US Department of Energy, March 2024. https://liftoff.energy.gov/wp-content/uploads/2024/03/LIFTOFF_Next-Generation-Geothermal-Power_Updated-2.5.25.pdf.

Bose, Anjan, Mark Lauby, et al. *Evolving Planning Criteria for a Sustainable Power Grid: A Workshop Report*. Atlanta: North American Electric Reliability Corporation; and Washington, DC: National Academy of Engineering, July 2024. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/Evolving_Planning_Criteria_for_a_Sustainable_Power_Grid.pdf.

Bowen, Thomas, Ilya Chernyakhovskiy, and Paul Denholm. *Grid-Scale Battery Storage: Frequently Asked Questions*. NREL/TP-6A20-74426. Golden, CO: National Renewable Energy Laboratory, September 2019. https://www.nrel.gov/docs/fy19osti/74426.pdf.

Boyd, Alex. "The Control Room Is at the Heart of the Energy Transition." *T&D World*, May 15, 2023. https://www.tdworld.com/smart-utility/article/21265807/the-control-room-is-at-the-heart-of-the-energy-transition

Bracken, Matt. "CISA Sees Increase in Zero-Day Exploitation, Official Says." *CyberScoop*, November 3, 2023. https://cyberscoop.com/cisa-zero-day-ransomware/.

Bright, Zach. "After Vogtle, What's Next for Nuclear?" *E&E News*, April 30, 2024. https://www.eenews.net/articles/after-vogtle-whats-next-for-nuclear/.

Brodt, Oleg. "A Brief History of ICS-Tailored Attacks." *Dark Reading*, August 31, 2023. https://www.darkreading.com/cyberattacks-data-breaches/brief-history-of-ics-tailored-attacks.

Bruzzese, Matt, and Peter W. Singer. "Farewell to China's Strategic Support Force. Let's Meet Its Replacements." *Defense One*, April 28, 2024. https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/.

Caddy, Cherylene, Edmon Begoli, Samuel Chanowski, Alexander Gates, Paul Stockton, and Virginia Wright. *Cybersecurity and Digital Components: Supply Chain Deep Dive Assessment: U.S. Department of Energy Response to Executive Order 14017, "America's Supply Chains."* Washington, DC: US Department of Energy, February 24, 2022. https://www.energy.gov/sites/default/files/2022-02/Cybersecurity%20Supply%20Chain%20Report%20-%20Final.pdf.

California Energy Commission. "Solar Equipment Lists." https://solarequipment.energy.ca.gov/Home/InverterSolarList.

———. "Solar Equipment Lists Program." https://www.energy.ca.gov/programs-and-topics/programs/solar-equipment-lists.

Campbell, Richard J. *Evolving Electric Power Systems and Cybersecurity*. CRS Report R46959. Washington, DC: Congressional Research Service, November 4, 2021. https://crsreports.congress.gov/product/pdf/R/R46959.

Carmakal, Charles, Sandra Joyce, Sunil Potti, Phil Venables, Willi Ballenthin, Dan Black, Sarah Bock, et al. *Cybersecurity Forecast 2024: Insights for Future Planning*. Mountain View, CA: Google, 2023. https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf.

Carnevale, Daniel, Mattia Cavaiola, and Andrea Mazzino. "A Novel AI-Assisted Forecasting Strategy Reveals the Energy Imbalance Sign for the Day-Ahead Electricity Market." *Energy Reports* 11 (2024): 4115–4126. https://doi.org/10.1016/j.egyr.2024.03.058.

Chandramowli, Shankar, Patty Cook, Justin Mackovyak, Himali Parmar, and Maria Scheller. *Power Surge: Navigating US Electricity Demand Growth*. Reston, VA: ICF, September 2024. https://www.icf.com/insights/energy/impact-rapid-demand-growth-us.

Chernicoff, David, and Matt Vincent. "Google and Amazon Make Major Inroads with SMRs to Bring Nuclear Energy to Data Centers." Data Center Frontier, October 16, 2024. https://www.datacenterfrontier.com/energy/article/55235902/google-and-amazon-make-major-inroads-with-smrs-to-bring-nuclear-energy-to-data-centers.

Choi, Charles Q. "EVs Are Essential Grid-Scale Storage." *IEEE Spectrum*, January 20, 2023. https://spectrum.ieee.org/electric-vehicle-grid-storage.

Choi, Seong. "Generative Artificial Intelligence for the Power Grid." National Renewable Energy Laboratory. https://www.nrel.gov/grid/generative-artificial-intelligence-for-the-power-grid.html.

Choi, Seong Lok, Rishabh Jain, Patrick Emami, Karin Wadsack, Fei Ding, Hongfei Sun, Kenny Gruchalla, Junho Hong, Hongming Zhang, Xiangqi Zhu, and Benjamin Kroposki. *eGridGPT: Trustworthy AI in the Control Room*. NREL/TP-5D00-87440. Golden, CO: National Renewable Energy Laboratory, May 2024. https://www.nrel.gov/docs/fy24osti/87740.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). "Alert Code AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." Last revised April 15, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

———. "Alert Code AA22-103A: APT Cyber Tools Targeting ICS/SCADA Devices." Last revised May 25, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a.

———. "Alert Code AA23-144a: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection." Released May 24, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

———. "Alert Code AA24-038A: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." Released February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

———. "Alert Code ICSA-22-055-03: Schneider Electric Energy." Last revised July 12, 2022. https://www.cisa.gov/news-events/ics-advisories/icsa-22-055-03.

———. "Alert: Supply Chain Compromise." Released January 7, 2021. https://www.cisa.gov/supply-chain-compromise.

———. "CISA and CNMF Analysis of SolarWinds-Related Malware." Last revised April 15, 2021. https://www.cisa.gov/news-events/alerts/2021/04/15/cisa-and-cnmf-analysis-solarwinds-related-malware.

———. "CISA Director Easterly's Remarks at the Atlantic Council: The Role of the Private Sector in Warfare." https://www.cisa.gov/cisa-director-easterlys-remarks-atlantic-council-role-private-sector-warfare.

———. *Cybersecurity Guidance: Chinese-Manufactured UAS*. Washington, DC: CISA, January 17, 2024. https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf.

———. *Electricity Sub-Sector Coordinating Council (ESCC) Charter*. May 2023. https://www.cisa.gov/sites/default/files/2023-09/energy-elec-scc-charter-May-2023-508_0.pdf.

———. *A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management*. Washington, DC: CISA, September 2023. https://www.cisa.gov/sites/default/files/2023-09/A%20Hardware%20Bill%20of%20Materials%20Framework%20for%20Supply%20Chain%20Risk%20Management%20%28508%29.pdf.

———. *Risk Assessment Methodologies*. Washington, DC: CISA. https://www.cisa.gov/sites/default/files/publications/Risk%2520Assessment%2520Methodologies.pdf.

———. "Traffic Light Protocol (TLP) Definitions and Usage." CISA blog, released August 16, 2022; revised August 22, 2022. https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.

CISA (Cybersecurity and Infrastructure Security Agency) et al. *Joint Cyber Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Product ID: AA24-038A. February 7, 2024. https://s3.documentcloud.org/documents/24412395/aa24-038a-csa-prc-state-sponsored-actors-compromise-us-critical-infrastructure.pdf.

CISA (Cybersecurity and Infrastructure Security Agency) et al. *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*. Washington, DC: CISA, October 25, 2023. https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.

CISA (Cybersecurity and Infrastructure Security Agency) et al. *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*. Washington, DC: CISA, April 13, 2023. https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf.

CISA and FBI (Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation). *Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure*. November 13, 2024. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications.

Colato, Javier, and Lindsey Ice. "Charging into the Future: The Transition to Electric Vehicles." *Beyond the Numbers: Employment & Unemployment* 12, no. 4 (2023). https://www.bls.gov/opub/btn/volume-12/charging-into-the-future-the-transition-to-electric-vehicles.htm.

Cooperative.com. "Electric Co-Ops and the Military." https://www.cooperative.com/programs-services/bts/cooperatives-and-the-military/Pages/default.aspx.

Copp, Tara. "An AI-Controlled Fighter Jet Took the Air Force Leader for a Historic Ride. What That Means for War." AP, May 3, 2024. https://apnews.com/article/artificial-intelligence-fighter-jets-air-force-6a1100c96a73ca9b7f41cbd6a2753fda.

Cory, Karlynn. "Behind-the-Meter Projects: Overview." Department of Energy *2020 Tribal Energy Webinar Series*, August 26, 2020. https://www.energy.gov/sites/prod/files/2020/08/f77/1_Cory-NREL.pdf.

CPUC (California Public Utilities Commission). *Working Group Report: Smart Inverter Operationalization Cybersecurity Subgroup (SIO-CS)*. San Francisco: CPUC, June 3, 2024. https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M532/K845/532845133.PDF.

Crossley, Cassie. *Software Supply Chain Security: Securing the End-to-End Supply Chain for Software, Firmware, and Hardware*. Sebastopol, CA: O'Reilly Media, March 2024.

Daniell, Amy. "Data Centers' Role in Providing Resilience and Flexibility to Power Grids." Data Centre Dynamics, July 2, 2024. https://www.datacenterdynamics.com/en/opinions/data-centers-role-in-providing-resilience-and-flexibility-to-power-grids/.

Danzig, Richard. *Technology Roulette: Managing Loss of Control as Many Militaries Pursue Technological Superiority*. Washington, DC: Center for a New American Security, June 2018. https://www.cnas.org/publications/reports/technology-roulette.

DARPA (Defense Advanced Research Projects Agency). "Rapid Attack Detection, Isolation and Characterization Systems (RADICS) (Archived)." https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems.

DCSA (US Defense Counterintelligence and Security Agency). "Foreign Ownership, Control or Influence." https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/.

Demeo, Anna. "Why We Need True AI-Driven Virtual Power Plants," February 9, 2024. Energy Changemakers. https://energychangemakers.com/ai-driven-virtual-power-plants/.

Dengler, Weston. "Pepco Manages Real-World Grid Complexity with Faster-than-Real-Time Simulation." *T&D World*, September 7, 2023. https://www.tdworld.com/overhead-distribution/article/21273193/pepco-manages-real-world-grid-complexity-with-faster-than-real-time-simulation.

Denholm, Paul, and Ben Kroposki. *Understanding Power Systems Protection in the Clean Energy Future*. Technical Report NREL/TP-6A40-82269. Golden, CO: National Renewable Energy Laboratory, May 2022. https://www.nrel.gov/docs/fy22osti/82269.pdf.

Derrick, Maya. "Top 10: Cloud Provider to the Energy Industry." *Energy Digital*, March 6, 2024. https://energydigital.com/top10/top-10-cloud-providers-to-the-energy-industry.

DHS (Department of Homeland Security). "Feature Article: Using Hydrogen to Power Disaster Relief." August 17, 2023. https://www.dhs.gov/science-and-technology/news/2023/08/17/feature-article-using-hydrogen-power-disaster-relief.

Di Bartolomeo, Mauricio. "Trump's Top 3 Bitcoin Promises and Their Implications." *Forbes*, November 7, 2024. https://www.forbes.com/sites/mauriciodibartolomeo/2024/11/07/trumps-top-3-bitcoin-promises-and-their-implications/.

DiGangi, Diana. "The AI Paradox: Energy-Hungry Technology Could Speed Clean Energy Transition." *Utility Dive*, December 10, 2024. https://www.utilitydive.com/news/artificial-intelligence-ai-data-center-energy-clean-transition-renewables/735061/.

———. "ENGIE Strikes Deal with Meta to Supply 260 MW of Solar." *Utility Dive*, October 31, 2024. https://www.utilitydive.com/news/engie-meta-solar-energy-data-center-purchase-agreement-power/731649/.

Di Giovanni, Fillipo. "Quantum Algorithms Will Optimize Grid Efficiency." *Power Electronics News*, June 13, 2024. https://www.powerelectronicsnews.com/quantum-algorithms-will-optimize-power-grid-efficiency/.

Dixon, Delaney, Cassie Powers, Jasmine McAdams, Sam Stephens, Danielle Sass Byrnet, and David Peters. *Mini Guide on Transportation Electrification: State-Level Roles and Collaboration among Public Utility Commissions, State Energy Offices, and Departments of Transportation*. Washington, DC: National Council on Electricity Policy, Summer 2022. https://pubs.naruc.org/pub/131FFF33-1866-DAAC-99FB-D86EE13B1709.

DOD (US Department of Defense). *Annual Energy Performance, Resilience, and Readiness Report: Fiscal Year 2023*. Washington, DC: DOD, July 29, 2024. https://www.acq.osd.mil/eie/eer/cr/ie/docs/aeprr/FY23-AEPRR-Report.pdf.

———. *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage*. Washington, DC: DOD, November 2, 2023. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

———. "Deputy Secretary of Defense Hicks Announces First Tranche of Replicator Capabilities Focused on All Domain Attritable Autonomous Systems." News release, May 6, 2024. https://www.defense.gov/News/Releases/Release/Article/3765644/deputy-secretary-of-defense-hicks-announces-first-tranche-of-replicator-capabil/.

———. *DOD Directive 3000.09: Autonomy in Weapon Systems*. Washington, DC: DOD, January 25, 2023. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

———. "Facility-Related Control Systems (FRCS) Cybersecurity." https://www.acq.osd.mil/eie/eer/cr/ie/frcs.html.

———. "Managing Cyber Risks to Facility-Related Control Systems." Memorandum February 18, 2020. https://www.acq.osd.mil/eie/eer/cr/ie/docs/frcs/Memo-on-Managing-Cyber-Risks-to-Fac-Related-Control-Systems.pdf.

———. *National Defense Industrial Strategy*. Washington, DC: DOD, January 11, 2024. https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf.

———. *National Defense Industrial Strategy Implementation Plan for FY2025*. Washington, DC: DOD, October 2024. https://www.businessdefense.gov/docs/ndis/NDIS-Implementation-Plan-FY2025.pdf.

———. *Notice of Availability of Designation of Chinese Military Companies*. 6001-FR, January 6, 2025. https://public-inspection.federalregister.gov/2025-00070.pdf.

———. *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review*. Washington, DC: DOD, October 27, 2022. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

DOD DSB (US Department of Defense Science Board). *Task Force on Cyber Deterrence*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017. https://apps.dtic.mil/sti/pdfs/AD1028516.pdf.

DOE (US Department of Energy). *Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investment Grant Program*. Washington, DC: DOE, September 2016. https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf.

———. "Artificial Intelligence Can Make the U.S. Electric Grid Smarter and More Reliable." Success Stories, Spotlight: Artificial Intelligence. September 2019. https://www.energy.gov/technologytransitions/articles/artificial-intelligence-can-make-us-electric-grid-smarter-and-more.

———. *Battery Energy Storge Systems Report*. Washington, DC: DOE, November 2024. https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf.

———. "Biden Administration, DOE to Invest $3 Billion to Strengthen U.S. Supply Chain for Advanced Batteries for Vehicles and Energy Storage." February 11, 2022. https://www.energy.gov/articles/biden-administration-doe-invest-3-billion-strengthen-us-supply-chain-advanced-batteries.

———. "Biden Administration Launches Bipartisan Infrastructure Law's $505 Million Initiative to Boost Deployment and Cut Costs of Increase Long Duration Energy Storage." May 12, 2022. https://www.energy.gov/articles/biden-administration-launches-bipartisan-infrastructure-laws-505-million-initiative-boost.

———. *Clean Energy Resources to Meet Data Center Electricity Demand*. August 12, 2024. https://www.energy.gov/policy/articles/clean-energy-resources-meet-data-center-electricity-demand.

———. *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*. Washington, DC: DOE, October 2022. https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf.

———. "DOE Announces $45 Million to Protect Americans from Cyber Threats and Improve Cybersecurity in America's Energy Sector." February 26, 2024. https://www.energy.gov/articles/doe-announces-45-million-protect-americans-cyber-threats-and-improve-cybersecurity.

———. "DOE Announces Nearly $23 Million to Bolster Energy Security and Resilience." September 26, 2024. https://www.energy.gov/ceser/articles/doe-announces-nearly-23-million-bolster-energy-security-and-resilience.

———. "DOE Cybersecurity Report Provides Recommendations to Secure Distributed Clean Energy on the Nation's Electricity Grid." October 6, 2022. https://www.energy.gov/eere/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy.

———. "Energy-Efficient Cooling Control Systems for Data Centers." https://www.energy.gov/eere/iedo/energy-efficient-cooling-control-systems-data-centers.

———. *Executive Summary: The National Transmission Planning Study*. Washington, DC: DOE, October 2024. https://www.energy.gov/sites/default/files/2024-10/NationalTransmissionPlanningStudy-ExecutiveSummary.pdf.

———. *The Future of Resource Adequacy: Solutions for Clean, Reliable, Secure, and Affordable Electricity*. Washington, DC: DOE April 2024. https://www.energy.gov/sites/default/files/2024-04/2024%20The%20Future%20of%20Resource%20Adequacy%20Report.pdf.

———. *The Future of Vehicle Grid Integration: Harnessing the Flexibility of EV Charging*. DOE/EE-2820. Washington, DC: DOE, July 2024. https://www.energy.gov/sites/default/files/2024-07/future-of-vehicle-grid-integration.pdf.

———. *Grid Security Emergency Orders: Procedures for Issuance*. *Federal Register*, vol. 83, no. 7, January 10, 2018. https://www.govinfo.gov/content/pkg/FR-2018-01-10/pdf/2018-00259.pdf.

———. "Grid Resilience and Innovation Partnerships (GRIP) Program, Technical Assistance Resource Center." https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center.

———. "Long Duration Storage Shot." https://www.energy.gov/eere/long-duration-storage-shot.

———. *Microgrid Overview*. Washington, DC: DOE, January 2024. https://www.energy.gov/sites/default/files/2024-02/46060_DOE_GDO_Microgrid_Overview_Fact_Sheet_RELEASE_508.pdf.

———. *National Cyber-Informed Engineering Strategy from the U.S. Department of Energy*. Washington, DC: DOE, June 2022. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf.

———. "Operation and Planning Tools for Inverter-Based Resource Management and Availability for Future Power Systems (OPTIMA) Funding Program." June 26, 2024. https://www.energy.gov/eere/solar/operation-and-planning-tools-inverter-based-resource-management-and-availability-future.

———. *Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure*. Washington, DC: US Department of Energy, April 2024. https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf.

———. *Power Grid and Communications Interdependencies: Key Challenges for Reliable, Resilient Operations*. Washington, DC: DOE, September 2003. https://www.energy.gov/sites/default/files/2023-10/Electric_Power_Telecommunications_Interdependencies_508.pdf.

———. "Powering On with Grid-Forming Inverters." January 4, 2021. https://www.energy.gov/eere/solar/articles/powering-grid-forming-inverters.

———. *Revocation of Prohibition Order Securing Critical Defense Facilities*. 6450-01-P. Washington, DC: DOE, April 20, 2021. https://www.energy.gov/sites/default/files/2021-04/Revocation%20of%20Prohibition%20Order%2004202021.pdf.

———. "Securing EV Charging Infrastructure Part 1: Why Cybersecurity Matters." April 10, 2024. https://www.energy.gov/ceser/articles/securing-ev-charging-infrastructure-part-1-why-cybersecurity-matters.

———. "Selected Projects for the Cyber Research, Development, and Demonstration Funding Opportunity." February 26, 2024. https://www.energy.gov/ceser/articles/selected-projects-cyber-research-development-and-demonstration-funding-opportunity.

———. *Secretarial Order: Unleashing the Golden Era of American Energy Dominance*. Washington, DC: DOE, February 5, 2025. https://www.energy.gov/articles/secretary-wright-acts-unleash-golden-era-american-energy-dominance.

———. *Solar Futures Study*. Washington, DC: DOE, September 2021. https://www.energy.gov/sites/default/files/2021-09/Solar%20Futures%20Study.pdf.

———. "Solar Integration: Inverters and Grid Services Basics." https://www.energy.gov/eere/solar/solar-integration-inverters-and-grid-services-basics.

———. "Solar Power Electronic Devices." https://www.energy.gov/eere/solar/solar-power-electronic-devices.

———. *Supply Chain Cybersecurity Principles*. Washington, DC: DOE, June 18, 2024. https://www.energy.gov/sites/default/files/2024-06/Final%20Supply%20Chain%20Cybersecurity%20Principles%20061424.pdf.

DOJ (US Department of Justice). "Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers." Press release, September 18, 2024. https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state.

———. "Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville." Press release, November 4, 2024. https://www.justice.gov/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility.

Donde, Vaibhav, Annabelle Pratt, Andrey Bernstein, Jack Flicker, Achintya Madduri, Ben Ollis, Ciaran Roberts, et al. *Microgrids as Building Blocks for the Future Grid—Topic 4*. Washington, DC: US Department of Energy, August 12, 2022. https://www.energy.gov/sites/default/files/2022-12/Topic4%20Report.pdf.

DOT (US Department of Transportation). "About ARPA-I." https://www.transportation.gov/arpa-i/about.

Downing, Jennifer, Nicholas Johnson, Mailinh McNicholas, David Nemtzow, Rima Oueid, Joseph Paladino, and Elizabeth Bellis Wolfe. *Pathways to Commercial Liftoff: Virtual Power Plants*. Washington, DC: US Department of Energy, September 2023. https://liftoff.energy.gov/wp-content/uploads/2023/09/20230911-Pathways-to-Commercial-Liftoff-Virtual-Power-Plants_update.pdf.

Dragos, Inc. "CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)." *The Dragos Blog*, April 13, 2022. https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/.

Dua, Shubhangi. "AI-Backed 'Self Healing' Tech Repairs Electric Grid Automatically." *Interesting Engineering*, June 25, 2024. https://interestingengineering.com/energy/ai-model-repairs-electric-grid-automatically.

EAC (Electricity Advisory Committee). *Enhancing Grid Resilience with Integrated Storage from Electric Vehicles: Recommendations for the U.S. Department of Energy*. Washington, DC: US Department of Energy, June 25, 2018, https://www.energy.gov/oe/articles/eac-recommendations-enhancing-grid-resilience-integrated-storage-electric-vehicles-june.

———. *Optimizing Reserves: Recommendations for the U.S. Department of Energy*. Washington, DC: US Department of Energy, October 2019. https://www.energy.gov/oe/articles/eac-optimizing-reserves-october-2019.

———. *Strengthening the Resilience of Defense Critical Electric Infrastructure: Recommendations for the U.S. Department of Energy*. Washington, DC: US Department of Energy, March 2022, https://www.energy.gov/sites/default/files/2022-03/EAC%20Recommendations%20-%20Strengthening%20DCEI%20Resilience%20-%20Final_508.pdf.

Easterly, Jen, and Jessica Rosenworcel. "The Most Important Part of the Internet You've Probably Never Heard Of." CISA blog, August 2, 2023. https://www.cisa.gov/news-events/news/most-important-part-internet-youve-probably-never-heard.

EIA (US Energy Information Administration). "Electricity Explained: Electricity in the United States." Last updated June 30, 2023. https://www.eia.gov/energyexplained/electricity/electricity-in-the-us.php#.

———. "Reserve Electric Generating Capacity Helps Keep the Lights On." *Today in Energy*, June 1, 2012. https://www.eia.gov/todayinenergy/detail.php?id=6510.

———. "Short-Term Energy Outlook." September 12, 2023. https://www.eia.gov/outlooks/steo/report/elec_coal_renew.php.

———. "Short-Term Energy Outlook." February 11, 2025. https://www.eia.gov/outlooks/steo/.

———. "What Is U.S. Electricity Generation by Energy Source?" Frequently Asked Questions (FAQs). February 2023. https://www.eia.gov/tools/faqs/faq.php?id=427&t=3.

Elliott, Rebecca F. "Three Mile Island, Notorious in Nuclear Power's Past, May Herald Its Future." *New York Times*, October 30, 2024. https://www.nytimes.com/2024/10/30/business/energy-environment/three-mile-island-nuclear-energy.html.

Energies Media Staff. "Why We Need AI-Driven Virtual Power Plants: A Step towards Sustainable Energy," April 3, 2024. Energies Media. https://energiesmagazine.com/why-we-need-ai-driven-virtual-power-plants-a-step-towards-sustainable-energy/.

Engle, John. "'Private Means Control:' Why Utilities Are Ditching Carriers for Their Own Private Communications Networks." Power Grid International, May 9, 2024. https://www.power-grid.com/td/communication-technology/private-means-control-why-utilities-are-ditching-carriers-for-their-own-communication-networks/.

EPRI (Electric Power Research Institute). *Advanced Metering Infrastructure (AMI) Risk Assessment and Security Requirements*. Palo Alto, CA: EPRI December 21, 2009. https://www.epri.com/research/products/000000000001017866.

———. "Electric Transportation." June 21, 2023. https://www.epri.com/portfolio/programs/053122.

———. *SOLAr Critical Infrastructure Energization (SOLACE): Leveraging Distributed Energy Resources to Provide Local Power*. Technical Update. Palo Alto, CA: EPRI, January 27, 2023. https://www.osti.gov/servlets/purl/1987533/.

———. "Transmission Planning." June 6, 2024. https://www.epri.com/portfolio/programs/027570.

ERCOT (Electric Reliability Council of Texas). *Ancillary Services*. Austin, TX: ERCOT, December 2023. https://www.ercot.com/files/docs/2023/06/06/Ancillary-Services-Handout-0524.pdf.

———. "ERCOT Creates Voluntary Curtailment Program for Large Flexible Customers During Peak Demand." News release, December 6, 2022. https://www.ercot.com/news/release/2022-12-06-ercot-creates-voluntary.

ESCC (Electricity Subsector Coordinating Council). "ESCC Overview." https://www.electricitysubsector.org/.

———. *The ESCC's Cyber Mutual Assistance Program*. May 2023. https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager.pdf?la=en&hash=827569B6061E85794AC581BF383C89E5D9DCD419.

Examining Emerging Threats to Electric Energy Infrastructure: Hearing Before the Subcommittee on Oversight and Investigations, U.S. House Committee on Energy and Commerce. 118th Cong. July 18, 2023. https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-examining-emerging-threats-to-electric-energy-infrastructure.

Executive Order 13920. *Securing the United States Bulk-Power System*. 85 FR 26595 (May 1, 2020). https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system.

Executive Order 14028. *Improving the Nation's Cybersecurity*. 86 FR 26633 (May 12, 2021). https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

Executive Order 14110. *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. 86 FR 75191 (November 1, 2023). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence#page-.

Executive Order 14154. *Unleashing American Energy*. 90 FR 8353 (January 20, 2022). https://www.federalregister.gov/documents/2025/01/29/2025-01956/unleashing-american-energy.

Executive Order 14156. *Declaring A National Energy Emergency*. 90 FR 8433 (January 20, 2025). https://www.federalregister.gov/documents/2025/01/29/2025-02003/declaring-a-national-energy-emergency.

FAA (Federal Aviation Administration). "UAS Detection and Mitigation Systems Aviation Rulemaking Committee." March 16, 2023. https://www.faa.gov/newsroom/uas-detection-and-mitigation-systems-aviation-rulemaking-committee-charter.

Fagan, Michael, Katerina Megas, Paul Watrobski, Jeffery Marron, and Barbara Cuthill. *Profile of the IoT Core Baseline for Consumer IoT Products*. NIST IR 8425. Gaithersburg, MD: National Institute of Standards and Technology, September 2022. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf.

Fasching, Elesia, and Suparna Ray. "More Than Half of New U.S. Electric-Generating Capacity in 2023 Will Be Solar." *Today in Energy*, February 26, 2023. https://www.eia.gov/todayinenergy/detail.php?id=55419#.

Federal Bureau of Investigation (FBI). "Expansion of US Renewable Energy Industry Increases Risk of Targeting by Malicious Actors." Private Industry Notification (PIN) 20240701-001. July 1, 2024. https://s3.documentcloud.org/documents/24788637/fbiwarning.pdf.

FCC (US Federal Communications Commission). *Protecting against National Security Threats to the Communications Supply Chain through FCC Programs—Huawei Designation*. FCC 20-179, Memorandum Opinion and Order. December 11, 2020. https://docs.fcc.gov/public/attachments/FCC-20-179A1.pdf.

FDA (US Food and Drug Administration). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff*. Silver Spring, MD: FDA, September 27, 2023. https://www.fda.gov/media/119933/download?attachment.

Feiner, Lauren. "Chinese Hackers Outnumber FBI Cyber Staff 50 to 1, Bureau Director Says." *CNBC*, April 28, 2023. https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html.

FERC (Federal Energy Regulatory Commission). *Energy and Ancillary Services Market Reforms to Address Changing System Needs*. September 2021. https://www.ferc.gov/sites/default/files/2021-09/20210907-4002_Energy%20and%20Ancillary%20Services%20Markets_2021_0.pdf.

———. *Explainer on the Inverter-Based Resources—Notice of Proposed Rulemaking*. October 2, 2024. https://www.ferc.gov/explainer-inverter-based-resources-notice-proposed-rulemaking.

———. *The February 2021 Cold Weather Outages in Texas and South Central United States: FERC, NERC and Regional Entity Staff Report*. November 16, 2021. https://www.ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and.

———. "FERC Order No. 2222: Fact Sheet." September 17, 2020. https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet#.

———. "FERC, NARUC Establish Federal-State Current Issues Collaborative." Press release, March 21, 2024. https://www.ferc.gov/news-events/news/ferc-naruc-establish-federal-state-current-issues-collaborative.

———. "FERC Proposes IBR Standards, Registration to Improve Grid Reliability." News release, November 17, 2022. https://www.ferc.gov/news-events/news/ferc-proposes-ibr-standards-registration-improve-grid-reliability.

———. *Final Rule: Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators*. Docket No. RM18-9-000, Order No. 2222. September 17, 2020. https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf.

———. *Final Rule: Reliability Standards to Address Inverter-Based Resources*. Docket No. RM22-12-000, Order No. 901. October 19, 2023. https://www.ferc.gov/media/e-1-rm22-12-000.

———. *Glossary*. https://www.ferc.gov/industries-data/market-assessments/overview/glossary.

———. *Incentives for Advanced Cybersecurity Investment*. Docket No. RM22-19-000; Order No. 893. April 21, 2023. https://www.ferc.gov/media/e-1-rm22-19-000-0.

———. *Notice of Proposed Rulemaking: Reliability Standards for Frequency and Voltage Protection Settings and Ride-Through for Inverter-Based Resources*. Docket No. RM25-3-000. December 19, 2024. https://www.ferc.gov/media/e-10-rm25-3-000.

———. *Notice of Proposed Rulemaking: Supply Chain Risk Management Reliability Standards Revisions*. Docket No. RM24-4-000. September 19, 2024. https://www.ferc.gov/media/e-1-rm24-4-000.

———. *Order Rejecting Amendments to Interconnection Service Agreement*. November 1, 2024. https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20241101-3061&optimized=false.

———. "Reliability Explainer." Last updated August 16, 2023. https://www.ferc.gov/reliability-explainer.

———. *Transcript | Technical Conference Regarding Large Loads Co-Located at Generating Facilities*. December 3, 2004. https://www.ferc.gov/media/transcript-technical-conference-regarding-large-loads-co-located-generating-facilities.

———. *2023 Lessons Learned from Commission-Led CIP Reliability Audits*. December 11, 2023. https://www.ferc.gov/sites/default/files/2023-12/23_Lessons%20Learned_1211.pdf.

FERC (Federal Energy Regulatory Commission) and E-ISAC (Electricity Information and Analysis Sharing Center). *SolarWinds and Related Supply Chain Compromise: TLP:WHITE—Lessons for the North American Electricity Industry*. Atlanta: North American Electric Reliability Corporation, April 15, 2021. https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf.

Ferreira, Summer, Murali Baggu, Russell Bent, Miguel Heleno, Tom King, Kevin Schneider, Ravindra Singh, and Vaibhav Donde. *DOE 2021 Strategy White Papers on Microgrids: Program Vision, Objectives, and R&D Targets in 5 and 10 Years—Topic Area #1*. Washington, DC: US Department of Energy, April 2021. https://www.energy.gov/sites/default/files/2022-12/Topic1%20Report.pdf.

Ferris, David. "Needed: Car Experts to Fend off Disaster." *E&E News*, June 12, 2023. https://www.eenews.net/articles/needed-car-experts-to-fend-off-grid-disaster.

Fix, Elliott, Abhishek Banerjee,Ulrich Muenz,and Gab-Su Seo. *Investigating Multi-Microgrid Black Start Methods Using Grid-Forming Inverters*. Preprint. Golden, CO: National Renewable Energy Laboratory, January 16, 2023, https://www.nrel.gov/docs/fy23osti/83956.pdf.

Forsyth, T., P. Tu, and J. Gilbert. "Economics of Grid-Connected Small Wind Turbines in the Domestic Market." NREL/CP-500-26975. Presented at the AWEA WindPower '99 Conference, Burlington, Vermont, June 20–23, 1999. https://www.nrel.gov/docs/fy00osti/26975.pdf.

Fortress Information Security. *A Software Supply Chain Dependent on Adversaries*. Orlando, FL: Fortress Information Security, December 4, 2023. https://www.fortressinfosec.com/en-usa-software-supply-chain-dependent-on-adversaries.

Fortune Business Insights. *U.S. Supercapacitor Market 2021–2028*. Market Research Report. Pune, India: Fortune Business Insights, January 2022. https://www.fortunebusinessinsights.com/u-s-supercapacitor-market-106291.

Gallagher, Mike, and Raja Krishnamoorthi. Letter to Jessica Rosenworcel, chair of the Federal Communications Commission, from chair (Gallagher) and ranking member (Krishnamoorthi) of the House Select Committee on the Chinese Communist Party. August 7, 2024, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2023-08-07-cellular-iot-modules.pdf.

GAO (US Government Accountability Office). *Information Environment: Opportunities and Threats to DOD's National Security Mission*. GAO-22-104714. Washington, DC: GAO, September 2022. https://www.gao.gov/assets/gao-22-104714.pdf.

Gellner, Jeffrey R., Curtis P. St. Michel, Sean McBride, and Micah Rich Steffensen. *Critical Function Assurance: Understanding Critical Function and Critical Function Delivery Is Foundational for Meaningful ICS Security Improvement and Policy Efforts*. INL/MIS-23-75497-Revision-0. Idaho Falls, ID: Idaho National Laboratory, November 2023. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_75387.pdf.

Gheorghiu, Iulia. "Congressman Targets Utility Security Clearances for New Legislation." *Utility Dive*, June 11, 2018, https://www.utilitydive.com/news/congressman-targets-utility-security-clearances-for-new-legislation/525374/.

Gimon, Eric. "Full Industrial Electrification Could More than Double US Power Demand. Here's How Renewables Can Meet It." *Utility Dive*, May 31, 2023. https://www.utilitydive.com/news/industrial-electrification-renewable-climate-energy-innovation/651572/.

GlobalData. "Artificial Intelligence: Who Are the Leaders in Electric Load Forecasting for the Power Industry?" *Power Technology*, September 25, 2024. https://www.power-technology.com/data-insights/innovators-ai-electric-load-forecasting-power/.

GlobalData. "Artificial Intelligence: Who Are the Leaders in Power Generation Forecasting for the Power Industry?" *Power Technology*, September 25, 2024. https://www.power-technology.com/data-insights/innovators-ai-power-generation-forecasting-power/.

Goldman Sachs. "AI Is Poised to Drive 160% Increase in Data Center Power Demand." *Insights*, May 14, 2024. https://www.goldmansachs.com/insights/articles/AI-poised-to-drive-160-increase-in-power-demand.

Goodin, Dan. "YubiKeys Are Vulnerable to Cloning Attacks Thanks to Newly Discovered Side Chanel." *Ars Technica*, September 3, 2024. https://arstechnica.com/security/2024/09/yubikeys-are-vulnerable-to-cloning-attacks-thanks-to-newly-discovered-side-channel/.

Gorman, Will, and Joachim Seel, eds. *Batteries Included: Top 10 Findings from Berkeley Lab Research on the Growth of Hybrid Power Plants in the United States*. Berkeley, CA: Lawrence Berkeley National Laboratory, April 19, 2022. https://eta-publications.lbl.gov/sites/default/files/berkeley_lab-_battery_included_-_top_10_hybrid_research.pdf.

Green, Alastair, Humayun Tai, Jesse Noffsinger, Pankaj Sachdeva, Arjita Bhan, and Raman Sharma. *How AI Data Centers and the Energy Sector Can Sate AI's Hunger for Power*. New York: McKinsey & Company, September 17, 2024. https://www.mckinsey.com/industries/private-capital/our-insights/how-data-centers-and-the-energy-sector-can-sate-ais-hunger-for-power.

GridScape. "The Symbiotic Role of Virtual Power Plants in Grid Stability." February 26, 2024. https://grid-scape.com/the-symbiotic-role-of-virtual-power-plants-in-grid-stability/.

GridWise Alliance. "GridWise Alliance Vision for an Integrated Grid." September 17, 2024. https://gridwise.org/the-gridwise-alliance-vision-for-an-integrated-grid/.

Gupta, Piyush. "AI in Demand Response: Future Energy Management." *FPGA Insights*, January 31, 2024. https://fpgainsights.com/power-management/ai-in-demand-response-future-energy-management/.

Gurzu, Anca. "Hackers Threaten Smart Power Grids." *Politico*, January 4, 2017. http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/.

Hadley, Greg. "In F-16 Dogfight, AI and Human Pilots Are 'Roughly an Even Fight,' Says Kendall." *Air & Space Forces Magazine*, May 8, 2024. https://www.airandspaceforces.com/kendall-ai-piloted-flight-embrace-autonomy/.

Halper, Evan. "Amid Explosive Demand, America Is Running Out of Power." *Washington Post*, March 7, 2024. https://www.washingtonpost.com/business/2024/03/07/ai-data-centers-power/.

Hansen, Aaron, Jason Staggs and Sujeet Shenoi. "Security Analysis of an Advanced Metering Infrastructure." *International Journal of Critical Infrastructure Protection* 18, no. C (2017): 3–19. https://doi.org/10.1016/j.ijcip.2017.03.004.

Hansen, Teresa. "GenAI: A Utility Disrupter and Enabler." *T&D World*, November 28, 2023. https://www.tdworld.com/smart-utility/article/21277454/generative-artificial-intelligence-a-utility-disrupter-and-enabler.

Hardikar, Aditi. Letter to Sherrod Brown and Tim Scott, Senate Committee on Banking, Housing, and Urban Affairs, December 30, 2024. https://www.documentcloud.org/documents/25473183-12/.

Hawaiian Electric. "Qualified Grid Support Utility Interactive Inverters and Controllers Meeting Mandatory Functions Specified in Rule 14H/IEEE1547-2018." October 4, 2023, last updated May 31, 2024. https://www.hawaiianelectric.com/documents/clean_energy_hawaii/qualified_equipment_list.pdf.

HCHS (US House Committee on Homeland Security). "WTAS: Joint Investigation into CCP-Backed Company Supplying Cranes to U.S. Ports Reveals Shocking Findings." March 12, 2024. https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings/.

Heckmann, Laura. "Indo-Pacific Command to Harness AI for Operational Planning." *National Defense*, March 25, 2024. https://www.nationaldefensemagazine.org/articles/2024/3/25/indo-pacific-command-to-harness-ai--for-operational-planning.

Heilweil, Rebecca. "OpenAI Further Expands Its Generative AI Work with the Federal Government." *FedScoop*, November 4, 2024. https://fedscoop.com/openai-expands-chatgpt-work-federal-government/.

Hoen, B. D., J. E. Diffendorfer, J. T. Rand, L. A. Kramer, C. P. Garrity, and H. E. Hunt. United States Wind Turbine Database v7.1, August 14, 2024. US Geological Survey, American Clean Power Association, and Lawrence Berkeley National Laboratory data release. https://doi.org/10.5066/F7TX3DN0.

Howe, Colleen. "Explainer: The Numbers behind China's Renewable Energy Boom." Reuters, November 15, 2023. https://www.reuters.com/sustainability/climate-energy/numbers-behind-chinas-renewable-energy-boom-2023-11-15/.

Howland, Ethan. "AEP, Others Press for FERC Guidance on 'Gargantuan' Issue of Data Center Colocation." *Utility Dive*, November 4, 2024. https://www.utilitydive.com/news/ferc-colocated-load-conference-resource-adequacy/731861/.

———. "Exelon's 'High Probability' Data Center Load Has Nearly Doubled to 11 GW, CEO Says." *Utility Dive*, October 31, 2024. https://www.utilitydive.com/news/exelon-data-center-load-co-location-pjm-capacity-earnings/731581/.

———. "Reregulation? How Utilities and States Are Responding to PJM's Record Capacity Prices." *Utility Dive*, September 4, 2024. https://www.utilitydive.com/news/pjm-capacity-auction-results-firstenergy-exelon-aep/725952/.

———. "Up to 58 GW Faces Retirement in PJM by 2030 Without Replacement Capacity in Sight: Market Monitor." *Utility Dive*, March 18, 2024. https://www.utilitydive.com/news/pjm-coal-gas-power-plant-risk-retirement-market-monitor/710518/.

Hughes, Chris, and Tony Turner. *Software Transparency: Supply Chain Security in an Era of a Software-Driven Society*. New York: Wiley, 2023.

Hutson, Matthew. "The Renewable-Energy Revolution Will Need Renewable Storage." *New Yorker*, April 18, 2022. https://www.newyorker.com/magazine/2022/04/25/the-renewable-energy-revolution-will-need-renewable-storage.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Washington, DC: Department of Homeland Security, September 16, 2016. https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

Idso, Shannon K., Francis K. Tuffner, Dexin Wang, Ryan Calkins, and Andrea Mammoli. *Port Electrification Handbook: A Reference to Aid U.S. Port Energy Transitions*. PNNL-36016. Richland, WA: Pacific Northwest National Laboratory, May 2024. https://www.pnnl.gov/projects/port-electrification-handbook.

IEEE. IEEE 1547-2018 (Revision of IEEE STD 1547-2003). *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.* Approved February 15, 2018; published April 6, 2018. https://standards.ieee.org/ieee/1547/5915/.

———. IEEE 1547.3-2023. *Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*. Approved June 5, 2023; published December 11, 2023. https://standards.ieee.org/ieee/1547.3/10173/.

———. IEEE P1547.3/D3.12. *IEEE Approved Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*. March 10, 2023. https://ieeexplore.ieee.org/document/10068352.

———. IEEE P2030.14. *Guide for Virtual Power Plant Functional Specification for Alternate and Multi-Source Generation*. PAR Approval June 29, 2023. https://standards.ieee.org/ieee/2030.14/11318/.

———. IEEE 2800-2022. *IEEE Standard for Interconnection and Interoperability of Inverter-Based Resources (IBRs) Interconnecting with Associated Transmission Electric Power Systems*. Approved February 9, 2022; published April 22, 2022. https://standards.ieee.org/ieee/2800/10453/.

———. IEEE 2413-2019. *IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*. Approved May 21, 2019; published March 10, 2020. https://standards.ieee.org/ieee/2413/6226/.

———. IEEE 2030.2.1-2019. *Guide for the Design, Operation, and Maintenance of Battery Energy Storage Systems, Both Stationary and Mobile, and Applications Integrated with Electric Power Systems*. Approved September 5, 2019; published December 13, 2019. https://standards.ieee.org/ieee/2030.2.1/5832/.

Igogo, Tsisilile, Paul Basore, Grant Bromhal, Samuel Browne, Cherylene Caddy, Gina Coplon-Newfield, Colin Cunliff, et al. *America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition: U.S. Department of Energy Response to Executive Order 14017, "America's Supply Chains."* Washington, DC: US Department of Energy, February 24, 2022. https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition.

INL (Idaho National Laboratory). "Cyber Testing for Resilient Industrial Control Systems™ (CyTRICS)." Fact Sheet. https://cytrics.inl.gov/cytrics/wp-content/uploads/2022/11/2022-05-04-CyTRICS-one-pg_formatted.pdf.

ISA (International Society of Automation). "ISA/IEC 62443 Series of Standards." https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Jankowski, Philip. "Demand from Large-Scale Users Could Strain Texas Power Grid, ERCOT Chief Says." *Dallas News*, April 24, 2024. https://www.dallasnews.com/news/politics/2024/04/24/demand-from-large-scale-users-could-strain-texas-power-grid-ercot-chief-says/.

Jennifer L. "U.S. Battery Storage Hits a New Record Growth in 2024." CarbonCredits.com, December 17, 2024. https://carboncredits.com/u-s-battery-storage-hits-a-new-record-growth-in-2024/.

Johnson, Jay, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, et al. *Cybersecurity for Electric Vehicle Charging Infrastructure*. Sandia Report SAND2022-9315. Albuquerque, NM: Sandia National Laboratories, July 2022. https://www.osti.gov/servlets/purl/1877784.

Johnson, Jay, Bheshaj Krishnappa, and Dan Goodlett. *Recommendations for Solar Energy Cybersecurity*. North American Electric Reliability Corporation, Solar Energy Industries Association, and Sandia National Laboratory, June 2023. https://www.nerc.com/pa/Documents/Recommendations-for-Solar-Energy-Cybersecurity.pdf.

Johnson, Jay, Jimmy Quiroz, Ricky Concepcion, Felipe Wilches-Bernal, and Matthew J. Reno. "Power System Effects and Mitigation Recommendations for DER Cyberattacks." *IET Cyber-Physical Systems: Theory and Applications* 4, no. 3 (2019): 240–249. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-cps.2018.5014.

Johnson, Jay, Timothy Berg, Benjamin Anderson, and Brian Wright. "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses." *Energies* 15, no. 11 (2022): article 3931. https://doi.org/10.3390/en15113931.

Joint Office of Energy and Transportation. "About." https://driveelectric.gov/#about-description.

Kahn, Ed. "Cooperation: The Key to Relay Protection Reliability." *T&D World*, July 7, 2023. https://www.tdworld.com/test-and-measurement/article/21264698/international-electrical-testing-association-cooperation-the-key-to-relay-protection-system-reliability.

Kahrl, Fredrich (Fritz), et al. *The Transition to a High-DER Electricity System: Creating A National Initiative on DER Integration for the United States*. Reston, VA: Energy Systems Integration Group August 2022. https://www.esig.energy/wp-content/uploads/2022/08/ESIG-DER-integration-US-initiative-report-2022.pdf.

Kashgar, Kasim. "World's Largest Drone Maker Expands in US amid Rights Abuse Allegations." *VOA*, March 14, 2024. https://www.voanews.com/a/world-s-largest-drone-maker-expands-in-us-amid-rights-abuse-allegations-/7526613.html.

Keller, J., and B. Kroposki. *Understanding Fault Characteristics of Inverter-Based Distributed Energy Resources*. Technical Report NREL/TP-550-46698. Golden, CO: National Renewable Energy Laboratory, January 2010. https://www.nrel.gov/docs/fy10osti/46698.pdf.

Khattak, Asad Masood, Salam Ismail Khanji, and Wajahat Ali Khan. "Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasures." In *Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019: Advances in Intelligent Systems and Computing*, vol. 935, edited by S. Lee, R. Ismail, and H. Choo. Cham: Springer, 2019. https://doi.org/10.1007/978-3-030-19063-7_44.

Krouse, Sarah, Robert McMillan, and Dustin Volz. "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack." *Wall Street Journal*, September 26, 2024. https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.

Kumar Maurya, Purushottam, Deepak A. Vidhate, Roshan Nayak, Pappula Madhavi, Pravin G.Gawande, and Eric Howard. "Self-Healing Grids: AI Techniques for Automatic Restoration after Outages." *Power Systems Technology* 48, no. 1 (March 2024): 494–510. https://powertechjournal.com/index.php/journal/article/view/302.

Lagos, Alex. "Winds of Change: The AI-Driven Evolution of DER Aggregators." Utility Analytics Institute, March 19, 2024. https://utilityanalytics.com/2024/03/ai-driven-evolution-of-der-aggregators/.

Lai, Christine, Nicholas Jacobs, Shamina Hossain-McKenzie, Cedric Carter, Patricia Cordeiro, Ifeoma Onunkwo, and Jay Johnson. *Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators*. Sandia Report SAND2017-13113. Albuquerque, NM: Sandia National Laboratory, December 17, 2017. https://sunspec.org/wp-content/uploads/2017/08/DERCyberPrimer-DraftforReview.pdf.

Larson, Aaron. "What Is DERMS and How Can It Help Utilities?" *POWER* Podcast, July 8, 2020. https://www.powermag.com/what-is-derms-and-how-can-it-help-utilities-podcast/.

Lauver, Madeline. "Cybersecurity Considerations for Electric Vehicle Chargers." *Security*, January 27, 2022. https://www.securitymagazine.com/articles/96989-cybersecurity-considerations-for-electric-vehicle-chargers.

Lawrence, Quil. "The Military Is Turning to Microgrids to Fight Global Threats—and Global Warming." *NPR*, October 2, 2023. https://www.npr.org/2023/10/02/1201838599/military-microgrids-climate-change.

Lawson, Ashley J. *Variable Renewable Energy: An Introduction*. In Focus IF11257. Washington, DC: Congressional Research Service, June 25, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11257.

LBNL (Lawrence Berkeley National Laboratory). "Grid Connection Requests Grow by 40% in 2022 as Clean Energy Surges, Despite Backlogs and Uncertainties." *Energy Markets & Policy*, April 4, 2023. https://emp.lbl.gov/news/grid-connection-requests-grow-40-2022-clean.

———. "Hybrid Power Plants: Status of Operating and Proposed Plants." *Energy Markets & Policy*. https://emp.lbl.gov/hybrid.

Linga, Vikram. "EIA Projects That Renewable Generation Will Supply 44% of U.S. Electricity by 2050." *Today in Energy*, March 18, 2022. https://www.eia.gov/todayinenergy/detail.php?id=51698.

Liou, Joanne. "What Are Small Modular Reactors (SMRs)?" International Atomic Energy Association, September 13, 2023. https://www.iaea.org/newscenter/news/what-are-small-modular-reactors-smrs.

Liu, Chen-Ching, Madhu Chinthavali, Rob Hovsapian, Hannah Burroughs, Sigifredo Gonzales, Francis K. Tuffner, Miguel Heleno, et al. *Topic 3: Building Blocks for Microgrids*. Washington, DC: Department of Energy, August 9, 2022. https://www.energy.gov/sites/default/files/2022-09/3-Building%20Blocks%20for%20Microgrids.pdf.

Lowder, Travis, and Kaifeng Xu. *The Evolving U.S. Distribution System: Technologies, Architectures, and Regulations for Realizing a Transactive Energy Marketplace*. NREL/TP-7A40-74412. Golden, CO: National Renewable Energy Laboratory, May 2020. https://www.nrel.gov/docs/fy20osti/74412.pdf.

Ludwigson, Jon, Raj Chitikila, Erin Carr, Megan Stewart, Lori Fields, Laura Greifner, Amanda Parker, Carrie Rogers, et al. *Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisition*. GAO-23-105850. Washington, DC: US Government Accountability Office, June 23, 2023. https://www.gao.gov/assets/gao-23-105850.pdf.

Lyu, Xue, and Jing Xie. *An Overview of Inverter-Based Resource Interconnection Standards*. Richland, WA: Pacific Northwest National Laboratory, November 2023. https://doi.org/10.2172/2217359.

Mahdavi, Meisam, Carlos Sabillon Antunez, Majid Ajalli, and Rubén Romero. "Transmission Expansion Planning: Literature Review and Classification." *IEEE Systems Journal* 13, no. 3 (2019): 3129–3140. https://doi.org/10.1109/Jsyst.2018.2871793.

Made-in-China. "Inverter." Product search results. https://www.made-in-china.com/products-search/hot-china-products/Inverter.html.

Mafazy, Midhat. *Paving the Way: Vehicle-to-Grid (V2G) Standards for Electric Vehicles*. Latham, New York: Interstate Renewable Energy Council, January 2022. https://irecusa.org/wp-content/uploads/2022/01/Paving_the_Way_V2G-Standards_Jan.2022_FINAL.pdf.

Mai, HJ. "Maryland Passes Energy Storage Pilot Program to Determine Future Regulatory Framework." *Utility Dive*, April 2, 2019. https://www.utilitydive.com/news/maryland-passes-energy-storage-pilot-program-to-determine-future-regulatory/551769/.

Mansour Saatloo, Amin, Arash Moradzadeh, Hamed Moayyed, Mostafa Mohammadpourfard, and Behnam Mohammadi-Ivatloo. "Hierarchical Extreme Learning Machine Enabled Dynamic Line Rating Forecasting." *IEEE Systems Journal* 16, no. 3 (2022): 4664–4674. https://doi.org/10.1109/JSYST.2021.3128213.

Martina, Michael. "Duke Energy Disconnects CATL Batteries from Marine Corps Base over Security Concerns." Reuters, December 7, 2023. https://www.reuters.com/world/us/duke-energy-disconnects-catl-batteries-marine-corps-base-camp-lejeune-2023-12-06/.

Matevosyan, Julia. *A Unique Window of Opportunity: Capturing the Reliability Benefits of Grid-Forming Batteries*. Reston, VA: Energy Systems Integration Group, March 2023. https://www.esig.energy/wp-content/uploads/2023/03/ESIG-GFM-batteries-brief-2023.pdf

Matre, Minal. *Harmonics in Photovoltaic Inverters & Mitigation Techniques*. Mumbai: Sterling and Wilson, December 2020. https://www.sterlingandwilsonre.com/images/knowledge-corner/pdfs/Harmonics%20in%20Photovoltaic%20Inverters%20&%20Mitigation%20Techniques.pdf.

Matz, Michael. "The Grid Is Moving to the Cloud." *EPRI Journal* 2021, no. 2 (2021): 15–16. https://eprijournal.com/the-grid-is-moving-to-the-cloud/.

———. "The Network Gateway: The Missing Link for Integrating Distributed Energy Resources?" *EPRI Journal* 2021, no. 1 (2021): 1–3. https://eprijournal.com/the-network-gateway-the-missing-link-for-integrating-distributed-energy-resources/.

Maxwell, Lauren. "Cyber Defense Agency: Threats Are Rising and Alaska Is Not Immune." *Alaska's News Source*, June 5, 2024. https://www.alaskasnewssource.com/2024/06/06/cyber-defense-agency-threats-are-rising-alaska-is-not-immune/.

Mazmanian, Adam. "Microsoft Deploys Air-Gapped AI for Classified Defense, Intelligence Customers." *NextGov/FWC*, May 7, 2024. https://www.nextgov.com/artificial-intelligence/2024/05/microsoft-deploys-air-gapped-ai-classified-cloud/396354/.

Mazzetti, Mark, and Edward Wong. "Inside U.S. Efforts to Untangle an A.I. Giant's Ties to China." *New York Times*, November 27, 2023; updated November 28, 2023. https://www.nytimes.com/2023/11/27/us/politics/ai-us-uae-china-security-g42.html.

McCarthy, James, Jeffrey Marron, Don Faatz, Daniel Rebori-Carretero, Johnathan Wiltberger, and Nik Urlaub. *Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems*. Initial Public Draft. NIST Interagency Report NIST IR 8498 ipd. Gaithersburg, MD: National Institute of Standards and Technology (NIST), May 2028. https://doi.org/10.6028/NIST.IR.8498.ipd.

McCarthy, Jim, Nakia Grayson, Joseph Brule, Tom Cottle, Alan Dinerman, John Dombrowski, Josie Long, Hillary Tran, Karen Quigg, Michael Thompson, Anne Townsend, and Nik Urlaub. *Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure*. NIST Interagency Report NIST IR 8473. Gaithersburg, MD: National Institute of Standards and Technology, October 2023. https://doi.org/10.6028/NIST.IR.8473.

McGready, Cy, Hatley Post, and Jane Nakano. "Energy Considerations at the Dawn of Strategic Manufacturing." CSIS, April 19, 2024. https://www.csis.org/analysis/energy-considerations-dawn-strategic-manufacturing.

McCurry, William. *State Energy Justice Roundtable Series: Customer Affordability and Arrearages*. Washington, DC: National Association of Regulatory Utility Commissioners, February 2023. https://pubs.naruc.org/pub/2B1596E2-1866-DAAC-99FB-37A81B4AFEF7?_gl=1*gexfr3*_ga*MTY2OTE0NTAyOS4xNzM3MjM5NDM0*_ga_QLH1N3Q1NF*MTczNzIzOTQzNC4xLjAuMTczNzIzOTQzNC4wLjAuMA.

McCurry, William, and Elliott Nethercutt. "Developing a Shared Framework to Value Resilience Investments." Chap. 2 in *Energy Resilience Reference Guide*. Washington, DC: National Association of Regulatory Utility Commissioners, February 2023. https://pubs.naruc.org/pub/458600D2-913F-CBF6-B8F3-BBF1A796F00E.

McDermott, Thomas E., Neil Shepard, Sakis Meliopoulos, Meghana Ramesh, Jeffrey D. Doty, and Jaime T. Kolln. *Protection of Distribution Circuits with High Penetration of Solar PV: Distance, Learning, and Estimation-Based Methods*. PNNL-32230. Richland, WA: Pacific Northwest National Laboratory, October 7, 2021. https://www.osti.gov/servlets/purl/1834373.

McFarland, Matt. "How a Battery Shortage Could Threaten US National Security." *CNN*, February 23, 2022. https://www.cnn.com/2022/02/22/cars/electric-vehicle-battery-supply-chain/index.html.

Miller, Nicholas W., and the Energy Systems Integration Group's Stability Task Force. *Diagnosis and Mitigation of Observed Oscillations in IBR-Dominant Power Systems: A Practical Guide*. Reston, VA: Energy Systems Integration Group, August 2024. https://www.esig.energy/wp-content/uploads/2024/08/ESIG-Oscillations-Guide-2024.pdf.

MISO (Midcontinent Independent System Operator). *MISO Operating Procedures*. Carmel, IN: MISO, September 20, 2018. https://efis.psc.mo.gov/Document/Display/9379.

Mohammadi, Ebrahim, Mojtaba Alizadeh, Mohsen Asgarimoghaddam, Xiaoyu Wang, and Marcelo Godoy Simões. "A Review on Application of Artificial Intelligence Techniques in Microgrids." *IEEE Journal of Emerging and Selected Topics in Industrial Electronics* 3, no. 4 (2022): 878–890. https://doi.org/10.1109/JESTIE.2022.3198504.

Mohan, Athira F., Nader Meskin, and Hasan Mehrjerdi. "A Comprehensive Review of the Cyber-Attacks and Cyber Security on Load Frequency Control of Power Systems." *Energies* 13, no. 15 (2020): article 3860. https://doi.org/10.3390/en13153860.

Morehouse, Catherine. "Congress, Texas Should 'Rethink' ERCOT's 'Go It Alone' Approach: FERC Chair Glick." *Utility Dive*, February 19, 2021. https://www.utilitydive.com/news/congress-texas-should-rethink-ercots-go-it-alone-approach-ferc-chair/595335/.

———. "Constellation to Restart Three Mile Island Nuclear Plant in Deal with Microsoft." *Politico*, September 20, 2024. https://www.politico.com/news/2024/09/20/constellation-nuclear-plant-deal-microsoft-00180218.

Moss, Sebastian. "NextEra Says There's 'Strong Interest' in Restarting Iowa Nuclear Plant for Data Centers." Data Centre Dynamics, October 23, 2024. https://www.datacenterdynamics.com/en/news/nextera-says-theres-strong-interest-in-restarting-iowa-nuclear-plant-for-data-centers/.

Muelaner, Jody. "Grid Frequency Stability and Renewable Power." Engineering.com, February 5, 2021. https://www.engineering.com/story/grid-frequency-stability-and-renewable-power.

Mukhina, Olena. "Decentralized Generation Network Is Long-Term Response to Russian Missile Attacks, Says Chief of Ukraine's State-Owned Grid Operator." *Euormaidan Press*, August 7, 2024. https://euromaidanpress.com/2024/08/07/decentralized-generation-network-is-long-term-response-to-russian-missile-attacks-says-chief-of-ukraines-state-owned-grid-operator/.

Muneer, Fowad, Joseph Adams, Shola Anjous, Amy Batallones, Dave Batz, Howard Biddle, Shawn Bilak, et al. *Cybersecurity Capability Maturity Model (C2M2)*. Version 2.1. Washington, DC: US Department of Energy, June 2022. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf.

Nadel, Steven. "Coming Electrification Will Require the Grid to Evolve." *ACEEE blog*, February 10, 2023. https://www.aceee.org/blog-post/2023/02/coming-electrification-will-require-grid-evolve.

Nakashima, Ellen, and Joseph Menn. "China's Cyber Army Is Invading Critical U.S. Services." *Washington Post*, December 11, 2023. https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/.

Narang, David. "Highlights of IEEE Standard 1547-2018." Webinar Presented to Arkansas DER Interconnection Stakeholders, October 18, 2018. https://www.nrel.gov/docs/fy20osti/75436.pdf.

NARUC (National Association of Regulatory Utility Commissioners). "Cybersecurity Baselines for Electric Distribution Systems and DER." https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/.

———. *Cybersecurity Baselines for Electric Distribution Utilities and DER: Draft Informative References*. Washington, DC: NARUC, February 2024. https://pubs.naruc.org/pub/364B7A14-D21C-D2DF-BB6B-FFF3F93E1D51.

———. *Cybersecurity Baselines for Electric Distribution Utilities and DER: Interim Implementation Guidance—Scope and Prioritization of the Baselines*. Washington, DC: NARUC, January 2025. https://www.energy.gov/sites/default/files/2025-01/Cybersecurity%20Baselines%20for%20Electric%20Distribution%20System%20Interim%20Implementation%20Guidance.pdf.

———. *Regulator's Financial Toolbox Brief: Operational Communications Networks for Grid Edge Technology Integration*. Washington, DC: NARUC. https://pubs.naruc.org/pub/524DEEAC-1866-DAAC-99FB-FA3CD3778E32.

———. "Reliability." https://www.naruc.org/serving-the-public-interest/about/reliability/.

———. *Resolution Recommending State Commissions Act to Adopt and Implement Distributed Energy Resource Standard IEEE 1547-2018*. Resolutions Proposed for Consideration at the 2020 NARUC Winter Policy Summit. February 12, 2020. https://pubs.naruc.org/pub/E86EF74B-155D-0A36-3138-B1A08D20E52B.

NASEM (National Academies of Sciences, Engineering, and Medicine). *The Future of Electric Power in the United States*. Washington, DC: National Academies Press, 2021. https://doi.org/10.17226/25968.

NATF (North American Transmission Forum). *Bulk Electric Systems Operations Absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Version 2.1, document ID: 1424. Charlotte, NC: North American Transmission Forum, February 23, 2024. https://www.natf.net/docs/natfnetlibraries/documents/resources/system-operations/bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach---open.pdf.

———. "The Industry Organizations Collaboration Effort." https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

———. *Supply Chain Security Assessment Model*. Version 2.1. Document ID: 1302. Charlotte, NC: NATF, October 23, 2023. https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/supply-chain-security-assessment-model.pdf.

National Grid ESO (Electricity System Operator). *Distributed ReStart: Final Findings and Proposals for Electricity System Restoration from DERs*. Warwick, UK: National Grid Electricity System Operator, October 2023. https://www.nationalgrideso.com/document/271831/download.

Naumann, Steven. *The Threat to the Electric Grid of Drones Must Be Analyzed and Action Taken Now*. Orlando, FL: Protect our Power, January 2023. https://protectourpower.org/wp-content/uploads/2023/01/PoP-Drones-Whitepaper-Jan-11.pdf

Nawy, Robert. "Electric Vehicles Are Taking Over. Hackers Are Waiting." *Security*, April 20, 2023. https://www.securitymagazine.com/articles/97461-electric-vehicles-are-taking-over-hackers-are-waiting.

NCSC (US National Counterintelligence and Security Center). *Safeguarding Our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies*. Washington, DC: NCSC, June 20, 2023. https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

NERC (North American Electric Reliability Corporation). "About Alerts." https://www.nerc.com/pa/rrm/bpsa/pages/about-alerts.aspx.

———. "About NERC." https://www.nerc.com/AboutNERC/Pages/default.aspx.

———. *Balancing and Frequency Control: Reference Document*. Atlanta: NERC, May 11, 2021. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reference_Document_NERC_Balancing_and_Frequency_Control.pdf.

———. *BAL-002-2 Background Document*. Atlanta: NERC, August 2014. https://www.nerc.com/pa/stand/project%202010141%20%20phase%201%20of%20balancing%20authority%20re/bal-002-2%20background%20document%20-%20clean%20-%202014%2006%2001.pdf.

———. *BAL-002-2—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Atlanta: NERC, August 2014. https://www.nerc.com/pa/stand/reliability%20standards/bal-002-2.pdf.

———. *BAL-002-3—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-3.pdf.

———.*BAL-002-WECC-3—ContingencyReserve*. https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-WECC-3.pdf.

———. *BAL-003-2—Frequency Response and Frequency Bias Setting*. Atlanta: NERC. https://www.nerc.com/pa/stand/reliability%20standards/bal-003-2.pdf.

———. *BES Operations in the Cloud: NERC Security Integration and Technology Enablement Subcommittee White Paper*. Atlanta: NERC, September 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SITES_WhitePaper_BES_Ops_in_Cloud.pdf.

———. *CIP-002-5.1a—Cyber Security—BES Cyber System Categorization*. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf.

———. *CIP-002-6—Cyber Security—BES Cyber System Categorization*. Redline to *CIP-005.1a*. https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP-002-6_Standard_redline_to_CIP-005.1a_09142017.pdf.

———. *CIP-013-2—Cyber Security—Supply Chain Risk Management*. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf.

———.*CIP-014-1—Physical Security.* https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-1.pdf.

———. *Cyber-Informed Transmission Planning: Roadmap for Integrating Cyber Security into Transmission Planning Activities*. Atlanta: NERC, May 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/ERO_Enterprise_Whitepaper_Cyber_Planning_2023.pdf.

———. *Cyber Security for Distributed Energy Resources and DER Aggregators: NERC Security Integration and Technology Enablement Subcommittee (SITES) White Paper*. Atlanta: NERC, December 6, 2022. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf.

———. *Distributed Energy Resources: Connection, Modeling, and Reliability Considerations*. Atlanta: NERC, February 2017. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/Distributed_Energy_Resources_Report.pdf.

———. *Electric Vehicle Dynamic Charging Performance Characteristics during Bulk Power System Disturbances*. Atlanta: NERC, April 2023. https://www.nerc.com/comm/RSTC/Documents/Grid_Friendly_EV_Charging_Recommendations.pdf.

———. *Electric Vehicle Task Force*. Atlanta: NERC, August 2024. https://www.nerc.com/comm/RSTC/EVTF/EVTF%20Scope.pdf.

———. *Energy Storage: Impacts of Electrochemical Utility-Scale Battery Energy Storage Systems on the Bulk Power System*. Atlanta: NERC, February 2021. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/Master_ESAT_Report.pdf.

———. *EOP-011-1 Emergency Operations*. https://www.nerc.com/pa/stand/reliability%20standards/eop-011-1.pdf.

———. *EOP-005-3—System Restoration from Blackstart Resources*. https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-005-3.pdf.

———. *Essential Actions to Industry: Cold Weather Preparations for Extreme Weather Events III*. Atlanta: NERC, May 15, 2023. https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/Level%203%20Alert%20Essential%20Actions%20to%20Industry%20Cold%20Weather%20Preparations%20for%20Extreme%20Weather%20Events%20III.pdf.

———. *Essential Reliability Services*. Atlanta: NERC. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/ERS%20Abstract%20Report%20Final.pdf.

———. *Essential Reliability Services: Whitepaper on Sufficiency Guidelines*. Atlanta: NERC, December 2016. https://nercstg.nerc.com/comm/Other/essntlrlbltysrvcstskfrcDL/ERSWG_Sufficiency_Guideline_Report.pdf.

———. *Frequently Asked Questions: Proposed Revisions to NERC Rules of Procedure to Address Registration of Owners and Operators of Unregistered Inverter-based Resources*. Atlanta: NERC, September 13, 2023. https://www.nerc.com/comm/RSTC/Documents/Frequently_Asked_Questions_-_Rules_of_Procedure_Approach_to_Registration_of_Unregistered_IBRs.pdf.

———. *Glossary of Terms Used in NERC Reliability Standards*. Atlanta: NERC, May 8, 2024. https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

———. *GridEx VI Lessons Learned Report*. Atlanta: NERC, April 2022. https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20VI%20Public%20Report.pdf.

———. *Grid Forming Technology: Bulk Power System Reliability Considerations*. Atlanta: NERC, December 2021. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Grid_Forming_Technology.pdf.

———. *An Introduction to Inverter-Based Resources on the Bulk Power System*. Atlanta: NERC, June 2023. https://www.nerc.com/pa/Documents/2023_NERC_Guide_Inverter-Based-Resources.pdf.

———. *An Introductory Guide to Electricity Markets Regulated by the Federal Energy Regulatory Commission*. Atlanta: NERC, last updated April 25, 2024. https://www.ferc.gov/introductory-guide-electricity-markets-regulated-federal-energy-regulatory-commission.

———. *Inverter-Based Resource Performance Issues Report: Findings from the Level 2 Alert*. Atlanta: NERC, November 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/NERC_Inverter-Based_Resource_Performance_Issues_Public_Report_2023.pdf.

———. *Joint Comments of the North American Electric Reliability Corporation and the Regional Entities in Response to Notice of Proposed Rulemaking*. Docket No. RM22-12-000, United States of America before the Federal Energy Regulatory Commission, February 6, 2023. https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Comments_IBR%20Standards%20NOPR.pdf.

———. Letter from Michael Assante, Chief Security Officer, on Critical Cyber Asset Identification, April 7, 2009. https://www.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf.

———. *Low Impact Criteria Review Report: NERC Low Impact Criteria Review Team White Paper*. Atlanta: NERC, October 2022. https://www.nerc.com/pa/Stand/Project%202023%2004%20Modifications%20to%20CIP%20003%20DL/NERC_LICRT_White_Paper_clean.pdf.

———. *North American Electric Reliability Corporation Five-Year Electric Reliability Organization Performance Assessment Report In Accordance With 18 C.F.R. § 39.3(c)*. Atlanta: NERC, July 19, 2024. https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Five%20Year%20Performance%20Assessment%202024%20Filing.pdf.

———. *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards BAL-007-1 and TOP-003-7*. Atlanta: NERC, January 6, 2025. https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20for%20Approval%20of%20Energy%20Assurance%20Standards_final_digicert.pdf.

———. *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards PRC-029-1 and PRC-024-4*. Atlanta: NERC, November 4, 2024. https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20for%20Appproval%20of%20PRC-029-1%20and%20PRC-024-4_digicert.pdf.

———. *Privacy and Security Impacts of DER and DER Aggregators; Joint SPIDERWG/SITES White Paper*. Atlanta: NERC, September 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/JointWhitePaper_PrivacyAndSecurityImpactsOfDERAggregators.pdf.

———. "Project 2006-03 System Restoration and Blackstart." https://www.nerc.com/pa/Stand/Pages/System_Restoration_Blackstart.aspx.

———. *Proposed Rule: Reliability Standards to Address Inverter-Based Resources*. December 6, 2022. https://www.federalregister.gov/documents/2022/12/06/2022-25599/reliability-standards-to-address-inverter-based-resources.

———. *Reliability Guideline: Bulk Power System Reliability Perspectives on the Adoption of IEEE 1547-2018*. Atlanta: NERC, March 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Guideline-IEEE_1547-2018_BPS_Perspectives_PostPubs.pdf.

———. *Reliability Guideline: Operating Reserve Management: Version 3*. Atlanta: NERC, June 8, 2021. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Template_Operating_Reserve_Management_Version_3.pdf.

———. *Reliability Guideline: Performance, Modeling, and Simulations of BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants*. Atlanta: NERC, June 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_BESS_Hybrid_Performance_Modeling_Studies.pdf.

———. *Reliability Terminology*. Atlanta: NERC, August 2013. https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf.

———. *Security Guideline for the Electricity Sector—Supply Chain: Risks Related to Cloud Service Providers*. Atlanta: NERC, December 10, 2019. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf.

———. *Severe Impact Resilience: Considerations and Recommendations*. Atlanta: NERC, May 2012. https://www.ourenergypolicy.org/wp-content/uploads/2012/05/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

———. *Short-Circuit Modeling and System Strength: White Paper*. Atlanta: NERC, February 2018. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/Short_Circuit_whitepaper_Final_1_26_18.pdf.

———. *Standard EOP-003-1—Load Shedding Plans*. Atlanta: NERC, January 1, 2007. https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-003-1.pdf.

———. *Standard PRC-006-2—Automatic Underfrequency Load Shedding*. Atlanta: NERC. https://www.nerc.com/pa/stand/reliability%20standards/prc-006-2.pdf.

———. *TPL-008-1—Transmission System Planning Performance Requirements for Extreme Temperature Events*. Atlanta: NERC, December 2024. https://www.nerc.com/pa/Stand/Project202307ModtoTPL00151TransSystPlanPerfReqExWe/2023-07_Final_Ballot_TPL-008-1_Standard_Clean_120224.pdf.

———. *2024 Long-Term Reliability Assessment*. Atlanta: NERC, December 2024. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Long%20Term%20Reliability%20Assessment_2024.pdf.

———. *2024 State of Reliability*. Atlanta: NERC, June 2024. https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2024_Technical_Assessment.pdf.

———. *2023 Long-Term Reliability Assessment*. Atlanta: NERC, December 2023. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2023.pdf.

———. *2023 ERO Reliability Risk Priorities Report*. Atlanta: NERC, July 24, 2023. https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC_ERO_Priorities_Report_2023_Board_Approved_Aug_17_2023.pdf.

———. *2023 State of Reliability Technical Assessment*. Atlanta: NERC, June 2023. https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Technical_Assessment.pdf.

———. *2023 Summer Reliability Assessment*. Atlanta: NERC, May 2023. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2023.pdf.

———. *2022 Long-Term Reliability Assessment*. Atlanta: NERC, December 2022. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2022.pdf.

———. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Report to the NERC Board of Trustees by the NERC Steering Group. Atlanta: NERC, July 13, 2004, https://www.nerc.com/pa/rrm/ea/August%2014%202003%20Blackout%20Investigation%20DL/NERC_Final_Blackout_Report_07_13_04.pdf.

———. *White Paper: Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems*. Atlanta: NERC, September 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_GFM_Functional_Specification.pdf.

Nevius, David. *The History of the North American Electric Reliability Corporation: Helping Owners, Operators, and Users of the Bulk Power System Assure Reliability and Security for More Than 50 Years*. 2nd ed. Atlanta: NERC, March 2020. https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf.

Nilsson, Henrik. "US Microgrid Market to Grow 19% Annually through 2027, Wood Mackenzie Projects." *Utility Dive*, February 8, 2023. https://www.utilitydive.com/news/us-microgrid-market-wood-mackenzie/642341/.

Ningbo Deye Inverter Technology Co. "Deye Has Launched New Firmware Version for Microinverter." February 8, 2023. https://www.deyeinverter.com/news/events-news/deye-has-launched-new-firmware-version-for-microinverter.html.

NIST (National Institute of Standards and Technology). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD: NIST, January 2023. https://doi.org/10.6028/NIST.AI.100-1.

———. *General Access Control Guidance for Cloud Systems*. NIST SP 800-210. Gaithersburg, MD: NIST, July 2020. https://csrc.nist.gov/pubs/sp/800/210/final.

———. *Glossary*. Last updated April 22, 2024. https://csrc.nist.gov/glossary.

———. "Software Security in Supply Chains: Software Bill of Materials (SBOM)." https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1.

NRC (Nuclear Regulatory Commission). "Common Cause Failure Definitions in Various Sources." Attachment to email from Mauricio R. Gutierrez, September 14, 2017. https://www.nrc.gov/docs/ML1725/ML17257A412.pdf.

NRECA (National Rural Electric Cooperatives Association). *Electric Co-Op Facts and Figures*. April 19, 2024. https://www.electric.coop/electric-cooperative-fact-sheet.

———. "What We Do." https://www.electric.coop/our-organization.

NREL (National Renewable Energy Laboratory). "Advanced Distribution Management Systems." https://www.nrel.gov/grid/advanced-distribution-management.html.

———. "Cybersecurity for Electric Vehicle Grid Integration." https://www.nrel.gov/transportation/electric-vehicle-grid-cybersecurity.html.

———. "Distributed Optimization and Control." https://www.nrel.gov/grid/distributed-optimization-control.html.

NSA (US National Security Agency). *2023 NSA Cybersecurity Year in Review*. Fort Meade, MD: NSA, December 19, 2023. https://media.defense.gov/2023/Dec/19/2003362479/-1/-1/0/NSA%202023%20Cybersecurity%20Year%20In%20Review.PDF.

NSCAI (National Security Commission on Artificial Intelligence). *Final Report*. March 19, 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

NYU (New York University). "Shock to the System: Electric Car Charging Stations May Be Portals for Power Grid Cyberattacks." Tandon School of Engineering press release, August 14, 2009. https://engineering.nyu.edu/news/shock-system-electric-car-charging-stations-may-be-portals-power-grid-cyberattacks.

O'Brien, Victoria. "Cybersecurity of Battery Energy Storage Systems." Presentation at the 2024 DOE Office of Electricity Energy Storage Program Annual Meeting, August 5, 2024. https://www.sandia.gov/app/uploads/sites/82/2024/08/PR2024_405_Obrien_Victoria_Regulatory.pdf.

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

Olivio, Antonio. "Internet Data Centers Are Fueling Drive to Old Power Source: Coal." *Washington Post*, April 17, 2024. https://www.washingtonpost.com/business/interactive/2024/data-centers-internet-power-source-coal/.

Osborne, Charlie. "CaddyWiper: More Destructive Wiper Malware Strikes Ukraine." *ZDNET*, March 15, 2022. https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/.

OSD (US Office of the Secretary of Defense). *Military and Security Developments Involving the People's Republic of China 2023: Annual Report to Congress*. Washington, DC: OSD, January 2023. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

Oxlee, Darren. "Cybersecurity Vital to Smart Metering Deployment." *Smart Energy International*, February 2019. https://www.smart-energy.com/digitalisation/cybersecurity/cybersecurity-vital-to-smart-metering-deployment/.

Pallardy, Richard. "AI Is Creating New Forms of Liability. How Can It Be Managed?" *Information Week*, October 8, 2024. https://www.informationweek.com/machine-learning-ai/ai-is-creating-new-forms-of-liability-how-can-it-be-managed-.

Palmer, Melissa. "Hyperscalers: The Complete Guide to What, Why and How." *Orange Matter*, January 24, 2023. https://orangematter.solarwinds.com/2023/01/24/hyperscalers-the-complete-guide/.

Peters, Keaton. "Texas Leaders Worry That Bitcoin Mines Threaten to Crash the State Power Grid." *Texas Tribune*, July 10, 2024. https://www.texastribune.org/2024/07/10/texas-bitcoin-mine-noise-power-grid-cryptocurrency/.

Petroc, Taylor. "Number of IoT Connections in North America in 2018, 2019 and 2025." Statista, January 18, 2023. https://www.statista.com/statistics/933099/iot-connections-north-america/.

PJM. "Ancillary Services Market." https://learn.pjm.com/three-priorities/buying-and-selling-energy/ancillary-services-market.

———. *BESS Technical Viability – Wagner and Brandon Shores Retirements: PJM Transmission and Operations Planning*. Audubon, PA: PJM, May 3, 2024. https://www.pjm.com/-/media/library/reports-notices/special-reports/2024/20240503-bess-technical-viability-wagner-and-brandon-shores-retirements-study.ashx.

———. *PJM Manual 13: Emergency Operation*s. Revision 88. Audubon, PA: PJM, May 18, 2023. https://www.pjm.com/-/media/DotCom/documents/manuals/archive/m13/m13v88-emergency-operations-05-18-2023.pdf.

———. *Energy Transition in PJM: Resource Retirements, Replacements & Risks*. Audubon, PA: PJM, February 24, 2023. https://www.pjm.com/-/media/library/reports-notices/special-reports/2023/energy-transition-in-pjm-resource-retirements-replacements-and-risks.ashx.

———. *Grid of the Future: PJM's Regional Planning Perspective*. Audubon, PA: PJM. https://pjm.com/-/media/library/reports-notices/special-reports/2022/20220510-grid-of-the-future-pjms-regional-planning-perspective.ashx.

———. *Winter Storm Elliott, Event Analysis and Recommendation Report*. Audubon, PA: PJM, July 17, 2023. https://pjm.com/-/media/library/reports-notices/special-reports/2023/20230717-winter-storm-elliott-event-analysis-and-recommendation-report.ashx.

Plautz, Jason. "As States Ramp Up Storage Targets, Policy Maneuvering Becomes Key." *Utility Dive*, February 8, 2023. https://www.utilitydive.com/news/as-states-ramp-up-storage-targets-policy-maneuvering-becomes-key/618218/.

Port of Long Beach. "Port Starts Construction on Microgrid Project." News release, March 8, 2022. https://polb.com/port-info/news-and-press/port-starts-construction-on-microgrid-project-03-08-2022/.

Port of Los Angeles. "Facts and Figures." https://www.portoflosangeles.org/business/statistics/facts-and-figures.

Portuondo, Nico. "Can Big Tech Revive Nuclear Power?" *E&E News*, October 28, 2024. https://www.eenews.net/articles/can-big-tech-revive-nuclear-power/.

Powering America's Economy, Security, and Our Way of Life: Examining the State of Grid Reliability: Hearing Before the Subcommittee on Energy, Climate, & Grid Security. 118th Cong., September 28, 2023. https://energycommerce.house.gov/events/energy-climate-and-grid-security-hearing-powering-america-s-economy-security-and-our-way-of-life-examining-the-state-of-grid-reliability.

Pratt, Alex. "Why AI and Distributed Energy Are Quietly Rescuing the Grid." *AutoGrid blog*, June 5, 2023. https://blog.auto-grid.com/why-ai-and-distributed-energy-are-quietly-rescuing-the-grid/.

Prengaman, Peter. "Ukraine Has Seen Success in Building Clean Energy, Which Is Harder for Russia to Destroy." Associated Press, November 20, 2024. https://apnews.com/article/ukraine-clean-renewable-energy-russian-bombing-distributed-1f226213742cc057f9f65208167e6f38.

Price, Hank. *Dispatchable Solar Power Plant Project*. Washington, DC: US Department of Energy, January 2018. https://www.osti.gov/biblio/1418902.

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler McLellan, and Chris Sistrunk. "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology." *Mandiant blog*, November 9, 2023. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/.

PS&C (Power Systems & Controls, Inc.). "What Is Power Quality." https://pscpower.com/what-is-power-quality/.

QED•C. *QuEnergy: Exploring the Role of Quantum Computing for the Electric Grid*. Arlington, VA: QED•C, November 28, 2022, https://quantumconsortium.org/quenergy22/.

Qui, Dawei, Goran Strbac, Yi Wang, Yujian Ye, Jiawei Wang, and Pierre Pinson. "Artificial Intelligence for Microgrid Resilience: A Data-Driven and Model-Free Approach." *IEEE Power & Energy Magazine* 22, no. 6 (November/December 2024): 18–27. https://doi.org/10.1109/MPE.2024.3405893.

Quimbre, Fiona, Ismael Arciniegas Rueda, Henri van Soest, Jon Schmid, Howard J. Shatz, Timothy R. Heath, Michal Meidan, et al. *China's Global Energy Interconnection: Exploring the Security Implications of a Power Grid Developed and Governed by China*. Santa Monica, CA: RAND Corporation, December 5, 2023. https://www.rand.org/pubs/research_reports/RRA2490-1.html.

Raman, Gururaghav, Bedoor AlShebli, Marcin Waniek, Talal Rahwan, and Jimmy Chih-Hsien Peng. "How Weaponizing Disinformation Can Bring Down a City's Power Grid." *PLoS ONE* 15, no. 8 (2020): article e0236517. https://doi.org/10.1371/journal.pone.0236517.

Ramasubramanian, Deepak. "Do We Have the Tools to Plan and Study IBR Oscillations during Interconnection?" *Proceedings of the ESIG Spring 2024 Technical Workshop*, March 28, 2024. https://www.esig.energy/event/2024-esig-g-pst-special-topic-workshop-a-deeper-look-at-oscillations/

Ray, Suparna, and Kristen Tsai. "Solar and Battery Storage to Make Up 81% of New US Electric Generating Capacity in 2024." *Today in Energy*, February 15, 2024. https://www.eia.gov/todayinenergy/detail.php?id=61424.

Ray, Suparna, and M. Tyson Brown. "U.S. Electricity Consumption by Light-Duty Vehicles Likely Surpassed Rail in 2023." *Today in Energy*, May 20, 2024; updated May 23, 2024. https://www.eia.gov/todayinenergy/detail.php?id=62083.

———. "Retirements of Electric Generating Capacity to Slow in 2024." *In-Brief Analysis*, February 2024. https://www.eia.gov/todayinenergy/detail.php?id=61425.

———. "U.S. Battery Storage Capacity Will Increase Significantly by 2025." *Today in Energy*, December 8, 2022. https://www.eia.gov/todayinenergy/detail.php?id=54939.

RFPB (Reserve Forces Policy Board) Subcommittee on the Reserve Component's Role in HD and Defense Support of Civil Authorities. *Reserve Component Support for Homeland Defense Report*. Washington, DC: RFPB August 27, 2024. https://rfpb.defense.gov/Portals/67/Documents/Reports/Cleared%20FINAL%20Consolidated%20RFPB%20HD%20REPORT%20pac.pdf.

Ribeiro, Anna. "China-Linked Hackers Allegedly Target US Internet Services in Salt Typhoon Attack." *Industrial Cyber*, September 26, 2024. https://industrialcyber.co/critical-infrastructure/china-linked-hackers-allegedly-target-us-internet-services-in-salt-typhoon-attack/.

The Role of Artificial Intelligence in Powering America's Energy Future: Hearing of the House Energy and Commerce Committee Subcommittee on Energy, Climate, and Grid Security United States House of Representatives. October 19, 2023. https://energycommerce.house.gov/events/energy-climate-and-grid-security-subcommittee-hearing-the-role-of-artificial-intelligence-in-powering-america-s-energy-future.

Rundle, James. "White House Takes Aim at Internet Security." *Wall Street Journal*, September 3, 2024. https://www.wsj.com/articles/white-house-takes-aim-at-internet-security-78103a69?mod=djemCybersecruityPro&tpl=cs.

Safder, Muhammad Umair, Mohammad J. Sanjari, Ameer Hamza, Rasoul Garmabdari, Md. Alamgir Hossain, and Junwei Lu. "Enhancing Microgrid Stability and Energy Management: Techniques, Challenges, and Future Directions." *Energies* 16, no. 18 (2023): article 6417. https://doi.org/10.3390/en16186417.

Sandalow, David, Michal Meidan, Philip Andrews-Speed, Anders Hove, Sally Qiu, and Edmund Downie. *Guide to Chinese Climate Policy 2022*. Oxford: Oxford Institute of Energy Studies, October 14, 2022. https://chineseclimatepolicy.oxfordenergy.org/.

Sanghvi, Anuj, and Tony Markel. "Cybersecurity for Electric Vehicle Fast-Charging Infrastructure." In *Proceedings of the 2021 IEEE Transportation Electrification Conference & Expo (ITEC)*, Chicago, IL, 2021, pp. 573–576, https://doi.org/10.1109/ITEC51675.2021.9490069.

Sawant, Jay, Gab-Su Seo, and Fei Ding. *Resilient Inverter-Driven Black Start with Collective Parallel Grid-Forming Operation*. Preprint. Golden, CO: National Renewable Energy Laboratory, January 16, 2023. https://www.nrel.gov/docs/fy23osti/83947.pdf.

Sayegh, Emil. "The Billion-Dollar AI Gamble: Data Centers as the New High-Stakes Game." *Forbes*, September 30, 2024. https://www.forbes.com/sites/emilsayegh/2024/09/30/the-billion-dollar-ai-gamble-data-centers-as-the-new-high-stakes-game/.

Schneider Electric. "TÜV Rheinland Certifies Schneider Electric's Secure Development Lifecycle Process to ISA/IEC 62443-4-1." Press release, October 22, 2019. https://www.se.com/ww/en/about-us/newsroom/news/press-releases/t%C3%BCv-rheinland-certifies-schneider-electric%E2%80%99s-secure-development-lifecycle-process-to-isa-iec-62443-4-1-5da9d78d8c5665197877d7c7.

Seals, Tara. "Critical Security Hole Can Knock Smart Meters Off Line." *Threatpost*, March 12, 2021. https://threatpost.com/critical-security-smart-meter-offline/164753/.

SEIA (Solar Energy Industries Association). "America Exceeds Five Million Solar Installations Nationwide." Press release, May 16, 2024. https://www.seia.org/news/5million.

———. "Utility-Scale Solar." https://seia.org/initiatives/utility-scale-solar/.

Seldin, Jeff. "US Defense Officials: China Is Leading in Hypersonic Weapons." *VOA*, March 10, 2023. https://www.voanews.com/a/us-defense-officials-china-is-leading-in-hypersonic-weapons/7000160.html.

Seiple, Chris. "Gridlock: The Demand Dilemma Facing the US Power Industry." Wood Mackenzie *Horizons*, October 2024. https://www.woodmac.com/horizons/gridlock-demand-dilemma-facing-us-power-industry/.

Shah, Jigar. "Introducing VPPieces: Bite-Sized Blogs about Virtual Power Plants." *VPPieces* (blog), US Department of Energy, May 12, 2022. https://www.energy.gov/lpo/articles/introducing-vppieces-bite-sized-blogs-about-virtual-power-plants.

Shepardson, David. "Trump Revokes Biden 50% EV Target, Freezes Unspent Charging Funds." Reuters, January 20, 2025. https://www.reuters.com/business/autos-transportation/trump-revokes-biden-order-that-set-50-ev-target-2030-2025-01-21/.

———. "Two Republicans Want Pentagon to Add Chinese Battery Maker CATL to Restricted List." Reuters, August 28, 2024. https://www.reuters.com/markets/two-republicans-want-pentagon-add-chinese-battery-maker-catl-restricted-list-2024-08-28/.

Shokry, Mostafa, Ali Ismail Awad, Mahmoud Khaled Abd-Ellah, and Ashraf A. M. Khalaf. "Systematic Survey of Advanced Metering Infrastructure Security: Vulnerabilities, Attacks, Countermeasures, and Future Vision." *Future Generation Computer Systems* 136 (2022): 358–377, https://doi.org/10.1016/j.future.2022.06.013.

Sigalos, MacKenzie, and Jordan Smith. "Texas Paid Bitcoin Miner Riot $31.7 Million to Shut Down during Heat Wave in August." *CNBC*, September 6, 2023. https://www.cnbc.com/2023/09/06/texas-paid-bitcoin-miner-riot-31point7-million-to-shut-down-in-august.html.

Singleton, Craig. *Beijing's Power Play: Safeguarding US National Security in the Electric Vehicle and Battery Industries*. Washington, DC: Foundation for Defense of Democracies, October 23, 2023. https://www.fdd.org/wp-content/uploads/2023/10/fdd-memo-beijings-power-play.pdf.

SNL (Sandia National Laboratories). "Cyber and Physical Security." https://energy.sandia.gov/programs/electric-grid/cyber-security-for-electric-infrastructure/.

———. "Artificial Intelligence and Machine Learning." https://energy.sandia.gov/programs/electric-grid/artificial-intelligence-and-machine-learning/.

SolarFix. "The Role of Firmware Updates in Solar Inverter Performance." *SolarFix blog*. https://solar-fix.com.au/blog/inverter-firemware-updates/.

S&P Global. "US Electric-Generating Capacity Retirements in 2024 to Be Lowest in 16 Years: EIA." *Commodity Insights*, February 20, 2024. https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/022024-us-electric-generating-capacity-retirements-in-2024-to-be-lowest-in-16-years-eia.

———. "US Has 133 New Gas-Fired Plants in The Works, Putting Climate Goals at Risk." May 15, 2024. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-has-133-new-gas-fired-plants-in-the-works-putting-climate-goals-at-risk-81469493.

Starks, Tim. "NSA Officials Call Out Chinese Hackers' Stealthy and Off-Limits Hacks." *Washington Post*, November 10, 2023. https://www.washingtonpost.com/politics/2023/11/10/nsa-officials-call-out-chinese-hackers-stealthy-off-limits-hacks/.

State of New Jersey. *2019 New Jersey Master Plan: Pathway to 2050*. https://nj.gov/emp/docs/pdf/2020_NJBPU_EMP.pdf.

Statista. "Electric Utilities in the U.S.—Statistics & Facts." https://www.statista.com/topics/2597/electric-utilities/#topicOverview.

Stern, David L. "Russia Destroyed Ukraine's Energy Sector, So Its Being Rebuilt Green." *Washington Post*, July 5, 2024. https://www.washingtonpost.com/world/2024/07/05/ukraine-green-power-rebuild-energy/.

St. John, Jeff. "Better Real-Time Data for the Country's Congested Transmission Lines." *Canary Media*, May 28, 2024. https://www.canarymedia.com/articles/transmission/better-real-time-data-for-the-countrys-congested-transmission-lines.

Strezoski, Luka, Harsha Padullaparti, Fei Ding, and Murali Baggu. "Integration of Utility Distributed Energy Resource Management System and Aggregators for Evolving Distribution System Operators." *Journal of Modern Power Systems and Clean Energy* 10, no. 2 (2022): 277–285. https://doi.org/10.35833/MPCE.2021.000667.

Stockton, Paul N. *Resilience for Grid Security Emergencies: Opportunities for Industry–Government Collaboration*. National Security Perspective NSAD-R-18-037. Laurel, MD: Johns Hopkins Applied Physics Laboratory, 2018. https://www.jhuapl.edu/sites/default/files/2022-12/ResilienceforGridSecurityEmergencies.pdf.

Stockton, Paul, Chris Beck, Michael Ross, Avi Schnurr, David Roop, Steven Naumann, Tom Galloway, Frank Koza, and Clayton Clem. *Electric Infrastructure Protection (EPRO®) Handbook V: Blackstart Power Restoration for a Greener Grid—Black Sky Resilience for a Changing Electric Grid Best Practices Handbook*. Washington, DC: Electric Infrastructure Security Council, 2024.

Sungrow. "Remote Firmware Upgrades via iSolarCloud." Hefei, China: Sungrow Power Supply Co. Ltd., 2020. https://www.sungrowpowerservice.com/Files/KnowledgeBase/Monitoring/TechDoc/GD_202010_iSolarCloud_Remote%20Firmware%20Upgrade_V1.0.pdf.

Sutter, Karen M. *"Made in China 2025" Industrial Policies: Issues for Congress*. CRS In Focus IF10964. Washington, DC: Congressional Research Service, updated March 10, 2023. https://sgp.fas.org/crs/row/IF10964.pdf.

Suvarna, Prakash, and Jeff Gooding. *Cyber-Intrusion Auto-Response and Policy Management System (CAPMS)*. Los Angeles: Southern California Edison, October 2015. https://www.sce.com/sites/default/files/inline-files/CyberIntrusionAutoResponse_PolicyManagement.pdf.

Tarafdar Hagh, Mehrdad, Mohammad Ali Jabbary Borhany, Kamran Taghizad-Tavana, and Morteza Zare Oskouei. "A Comprehensive Review of Flexible Alternating Current Transmission System (FACTS): Topologies, Applications, Optimal Placement, and Innovative Models." *Heliyon* 11, no. 1 (2025): e41001. https://doi.org/10.1016/j.heliyon.2024.e41001.

T&D World Staff. "Avangrid Pilots Mobile Robot Dog to Advance Substation Inspections with Artificial Intelligence." *T&D World*, February 12, 2024. https://www.tdworld.com/substations/article/21282583/avangrid-pilots-mobile-robot-dog-to-advance-substation-inspections-with-artificial-intelligence.

———. "FirstEnergy Deploys AI-Driven Program to Predict and Reduce Tree-Related Outages." *T&D World*, October 11, 2024. https://www.tdworld.com/vegetation-management/news/55234813/firstenergy-deploys-ai-driven-program-to-predict-and-reduce-tree-related-outages.

———. "How Artificial Intelligence Is Dramatically Impacting Energy Forecasting." *T&D World*, June 11, 2024. https://www.tdworld.com/smart-utility/whitepaper/55082411/how-artificial-intelligence-is-dramatically-impacting-energy-forecasting.

———. "Southern Company and Ford Pro Partner on 6-Month EV Fleet Grid-Enhancing Pilot Program." *T&D World*, December 20, 2024. https://www.tdworld.com/electrification/news/55251271/southern-company-and-ford-pro-partner-on-6-month-ev-fleet-grid-enhancing-pilot-program.

Texas RE. "Registration and Certification." https://www.texasre.org/registration.

Tietjen, Darryl. "Tariff Development I: The Basic Ratemaking Process." Rate Case Training, National Association of Regulatory Utility Commissioners. https://pubs.naruc.org/pub.cfm?id=538E730E-2354-D714-51A6-5B621A9534CB.

Timberlake, Laura. "Hackers Target HVAC." *HVAC News*, June 30, 2020. https://www.hvacrnews.com.au/news/hackers-in-hvac/.

Toohey, Grace, and Alexandra E. Petri. "A Text Asked Millions of Californians to Save Energy. They Paid Heed, Averting Blackouts." *Los Angeles Times*, September 7, 2022. https://www.latimes.com/california/story/2022-09-07/a-text-asked-millions-of-californians-to-save-energy-they-listened-averting-blackouts.

UL. *PV Inverter and BESS Converters Certification*. https://www.ul.com/services/pv-inverter-certification.

———. UL 2941: *UL LLC Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources*. Published January 13, 2023; last revised June 14, 2024. https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941.

UNIFI Consortium. *UNIFI Specifications for Grid-Forming Inverter-Based Resources*. Version 2. UNIFI-2024-2-1. March 2024. https://www.nrel.gov/docs/fy24osti/89269.pdf.

Toews, Rob. "AI That Can Invent AI Is Coming. Buckle Up." *Forbes*, November 3, 2024. https://www.forbes.com/sites/robtoews/2024/11/03/ai-that-can-invent-ai-is-coming-buckle-up/.

Trabish, Herman K. "As Reliability Concerns with Renewables Rise, Upgrading Inverters Is Urgent, Analysts Say." *Utility Dive*, January 2, 2024. https://www.utilitydive.com/news/grid-forming-inverters-vital-protect-the-grid-solar-wind-batteries/702892/.

Tucci, Bryana. "AWS Marketplace Now Available in the AWS Secret Region." *AWS Public Sector Blog*, January 26, 2024. https://aws.amazon.com/blogs/publicsector/aws-marketplace-now-available-in-the-aws-secret-region/.

Tuladhar, L. R., and K. Banerjee. *Impact of the Penetration of Inverter-Based Systems on Grid Protection*. Paris: CIGRE, 2019. https://cigre-usnc.org/wp-content/uploads/2019/10/2D_3.pdf.

Uberti, David. "There's Not Enough Power for America's High-Tech Ambitions." *Wall Street Journal*, May 12, 2024. https://www.wsj.com/business/energy-oil/data-centers-energy-georgia-development-7a5352e9?mod=hp_lead_pos7.

UL Solutions. "UL Solutions and NREL Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification." April 18, 2023. https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity.

University of Tennessee. "Superbowl Frequency Swings." Power Information Technology Laboratory study. https://powerit.utk.edu/frequency_swings.html.

USCC (US China Economic and Security Review Commission). "Section 3: China's Energy Plans and Practices." In *2022 Report to Congress*, 234–290. Washington, DC: USCC, November 2022. https://www.uscc.gov/sites/default/files/2022-11/Chapter_2_Section_3--Chinas_Energy_Plans_and_Practices.pdf.

USCYBERCOM. "USCYBERCOM Unveils AI Roadmap for Cyber Operations." News release, September 13, 2024. https://www.cybercom.mil/Media/News/Article/3905064/uscybercom-unveils-ai-roadmap-for-cyber-operations/.

VanHerck, Glen D., and Jacqueline D. Van Ovost. "Fighting to Get to the Fight." *Military Times*, May 31, 2022. https://www.militarytimes.com/opinion/commentary/2022/05/31/fighting-to-get-to-the-fight/.

Veritone. "Artificial Intelligence Power Grids and Autonomous Network Management." Smart Grids series, *Veritone blog*. https://www.veritone.com/blog/artificial-intelligence-power-grids-and-autonomous-network-management/.

Vicens, A. J. "Easterly: Potential Chinese Cyberattack Could Unfold Like CrowdStrike Error." *CyberScoop*, August 7, 2024. https://cyberscoop.com/easterly-crowdstrike-china-volt-typhoon/.

Vincent, Brandi. "Scale AI Unveils 'Defense Llama' Large Language Model for National Security Users." *DefenseScoop*, November 4, 2024. https://defensescoop.com/2024/11/04/scale-ai-unveils-defense-llama-large-language-model-llm-national-security-users/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru.

Violino, Bob. "How AI and Better Pay Can Address the Ongoing Cyber Talent Shortage." *CNBC*, September 27, 2023. https://www.cnbc.com/2023/09/27/how-ai-and-better-pay-can-address-the-ongoing-cyber-talent-shortage.html.

Walton, Rod. "AI Aims for Real: Artificial Intelligence and Its Role in the Microgrid-Distributed Energy Future." *Microgrid Knowledge*, October 6, 2023. https://www.microgridknowledge.com/artificial-intelligence/article/33012742/making-data-work-artificial-intelligence-will-change-the-microgrid-future-forever.

———. "EIA Prepares for Second Attempt to Survey Bitcoin Miners about Electricity Consumption." *Utility Dive*, July 11, 2024. https://www.utilitydive.com/news/federal-government-prepares-second-attempt-to-survey-bitcoin-miners-energy-se/721063/.

———. "EPRI Launches Data Center Flexibility Initiative with Utilities, Google, Meta, NVIDIA." *Utility Dive*, October 30, 2024. https://www.utilitydive.com/news/epri-launches-data-center-flexibility-initiative-with-NVIDIA-google-meta/731490/.

———. "'Explosive' Demand Growth Puts More Than Half of North America at Risk of Blackouts: NERC. *Utility Dive*, December 18, 2024. https://www.utilitydive.com/news/explosive-demand-growth-blackouts-NERC-LTRA-reliability/735866/.

———. "NERC Finding 25% of Utilities Exposed to SolarWinds Hack Indicates Growing ICS Vulnerabilities, Analysts Say." *Utility Dive*, April 15, 2021. https://www.utilitydive.com/news/nerc-finding-25-of-utilities-exposed-to-solarwinds-hack-indicates-growing/598449/.

———. "NERC Wary of 100 GW on Possible Plant Retirements and Other Takeaways from CEO Jim Robb." *Utility Dive*, July 26, 2024. https://www.utilitydive.com/news/5-takeaways-from-jim-robbs-wires-address-NERC/722486/.

———. "9 US Electric Power Sector Issues to Watch in 2025." *Utility Dive*, January 8, 2025. https://www.utilitydive.com/news/electric-power-sector-issues-to-watch-prices-demand-reliability-renewables-nuclear-vpp-transmission/736492/.

WECC (Western Electricity Coordinating Council). *Western Assessment of Resource Adequacy*. Salt Lake City: Western Electricity Coordinating Council, November 2022. https://www.wecc.org/Reliability/2022%20Western%20Assessment%20of%20Resource%20Adequacy.pdf.

Welch, Charley. "CYBERCOM's New AI Task Force Working Under 'Elite' Defensive Operations Unit." *Breaking Defense*, July 31, 2024. https://breakingdefense.com/2024/07/cybercoms-new-ai-task-force-working-under-elite-defensive-operations-unit/.

Wendel, JoAnna. "ChatGrid™: A New Generative AI Tool for Power Grid Visualization." News release, Pacific Northwest National Laboratory, February 22, 2024. https://www.pnnl.gov/news-media/chatgridtm-new-generative-ai-tool-power-grid-visualization.

Wheaton, Grace, and Corrina Ricker. "U.S. Natural Gas-Fired Electricity Generation Set New Daily Records in Summer 2024." *In-Brief Analysis*, October 8, 2024. https://www.eia.gov/todayinenergy/detail.php?id=63404.

White House. *Energy Modernization Cybersecurity Implementation Plan*. December 2024. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/12/Energy-Modernization-Cybersecurity-Implementation-Plan.pdf.

———. *Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports*. February 21, 2024. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/.

———. *Fact Sheet: Biden-Harris Administration Announces Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future*. August 9, 2024. https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/08/09/fact-sheet-biden-harris-administration-announces-priorities-for-enhancing-the-digital-ecosystem-to-support-a-secure-energy-future/.

———. *Fact Sheet: President Donald J. Trump Takes Action to Enhance America's AI Leadership*. January 23, 2025. https://www.whitehouse.gov/briefings-statements/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/.

———. *Fact Sheet: Protecting America from Connected Vehicle Technology from Countries of Concern*. September 23, 2024. https://www.presidency.ucsb.edu/documents/fact-sheet-protecting-america-from-connected-vehicle-technology-from-countries-concern.

———. *Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence*. October 24, 2024. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/.

———. *National Security Memorandum on Critical Infrastructure Security and Resilience*. NSM-22. April 30, 2024. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

———. *Readout of White House Roundtable on U.S. Leadership in AI Infrastructure*. Statement/release, September 12, 2024. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/09/12/readout-of-white-house-roundtable-on-u-s-leadership-in-ai-infrastructure/.

———. *Statement from National Security Advisor Jake Sullivan on the Global Effort to Strengthen the Cybersecurity of Energy Supply Chains*. June 18, 2024. https://www.presidency.ucsb.edu/documents/statement-national-security-advisor-jake-sullivan-the-global-effort-strengthen-the.

———. "Statement from President Biden on Addressing National Security Risks to the U.S. Auto Industry." Statements and releases, February 29, 2024. https://www.govinfo.gov/content/pkg/DCPD-202400146/pdf/DCPD-202400146.pdf.

———. *Temporary Withdrawal of All Areas on the Outer Continental Shelf from Offshore Wind Leasing and Review of the Federal Government's Leasing and Permitting Practices for Wind Projects*. Memorandum for the Secretary of the Treasury, the Attorney General, the Secretary of the Interior, the Secretary of Agriculture, the Secretary of Energy, and the Administrator of the Environmental Protection Agency, January 20, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/temporary-withdrawal-of-all-areas-on-the-outer-continental-shelf-from-offshore-wind-leasing-and-review-of-the-federal-governments-leasing-and-permitting-practices-for-wind-projects/.

Wilson, John D., and Zach Zimmerman. "The Era of Flat Power Demand Is Over." Bethesda, MD: Grid Strategies, December 2023. https://gridstrategiesllc.com/wp-content/uploads/2023/12/National-Load-Growth-Report-2023.pdf.

Wolf, Gene. "Microgridation Is Changing the Power Grid." *T&D World*, August 23, 2023. https://www.tdworld.com/distributed-energy-resources/article/21271684/microgridation-is-changing-the-power-grid.

Xu, Chjengian, Paul Behrens, Paul Gasper, Kandler Smith, Mingming Hu, Arnold Tukker, and Bernhard Steubing. "Electric Vehicle Batteries Alone Could Satisfy Short-Term Grid Storage Demand by as Early as 2030." *Nature Communications* 14 (2023): article 119. https://doi.org/10.1038/s41467-022-35393-0.

Yajun Wang, Hung-Ming Chou, Rui Sun, Wenyun Ju, Chetan Mishra, and Kyle Thomas. "Dynamic Study of Dominion's System Restoration Plan in RTDS." In *Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. Piscataway, NJ: IEEE, 2019. https://doi.org/10.1109/ISGT.2019.8791601.

Yu, Nanpeng. "Machine Learning Solutions for Monitoring U.S. Transmission Grid with Largescale Real-World PMU Data." Presented at the Fifth Workshop on Autonomous Energy Systems, July 15, 2022. https://www.nrel.gov/grid/assets/pdfs/2022aes-yu-machine-learning-solutions.pdf.

Acknowledgments

My special thanks go to David Batz (managing director, cyber and infrastructure security, Edison Electric Institute) and Steve Naumann (former vice president for transmission, Exelon), who generously shared their time and expertise through multiple study drafts. I also thank the following colleagues for their many contributions and edits: Victor Atkins, Burns & McDonnell; Wayne Austad, Idaho National Laboratory (INL); Jonathan Bransky, Dominion Energy; Daniel Brooks, Electric Power Research Institute (EPRI); Cheri Caddy, McCrary Institute for Cyber & Critical Infrastructure Security; Stan Connally Jr., Southern Company; Lynn Costantini, National Association of Regulatory Utility Commissioners (NARUC); Mark Gabriel, United Power; Tom Galloway, North American Transmission Forum (NATF); Matt Gardner, Dominion Energy; Howard Gugel, North American Electric Reliability Corporation (NERC); Brian Harrell, Avangrid; Lance LaBreck, California Independent System Operator (CAISO); Mark Lauby, NERC; Todd Lucas, Southern Company; Steve McElwee, PJM; Jonathon Monken, Converge Strategies; Richard Mroz, former president of the New Jersey Board of Public Utilities; Thomas O'Brien, PJM; Jim Robb, NERC; Dave Roop, former manager of Dominion Energy Virginia's electric transmission operations and reliability organization; Brian Seal, EPRI; Emma Stewart, INL; Andrea Sultana, ANSER; Christopher Wakefield, Southern Company; Matt Wakefield, EPRI; Bruce Walker, Pacific Northwest National Laboratory (PNNL); and Virginia Wright, INL. I also thank the many additional industry and government reviewers who prefer to remain anonymous. The findings and recommendations in the study are my own, however, and do not represent the policies of any of the organizations with which my reviewers are affiliated.

I would also like to thank my current and former colleagues at APL for their invaluable insights and editorial support: Richard Danzig; Andrew Mara; James Miller; Catherine Peacock; Erin Richardson; Matt Schaffer; Rob Schrier; and Paul Velez.

The views expressed in this article are those of the author and do not reflect the official policy of the Department of Defense or the US government.

About the Author

Paul Stockton is a senior fellow of the Johns Hopkins Applied Physics Laboratory (APL) and leads Paul N. Stockton LLC, a strategic advisory firm in Santa Fe, New Mexico. He previously served as the managing director of Sonecon LLC and was the assistant secretary of defense for homeland defense and Americas' security affairs from May 2009 until January 2013. In his current capacity, Dr. Stockton helps the electric industry strengthen preparedness against emerging cyber threats. He chairs the Grid Resilience for National Security subcommittee of DOE's Electricity Advisory Committee and the Homeland Defense subcommittee of DOD's Reserve Forces Policy Board. He also assists with cybersecurity initiatives for the water and wastewater sector. Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of

the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, the department's highest civilian award. The Department of Homeland Security awarded him its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Resilience for Grid Security Emergencies: Opportunities for Industry–Government Collaboration* (Laurel, MD: APL, 2018) and numerous other publications. He served as the facilitator of the GridEx IV and V exercises (2017 and 2019, respectively) and is a member of the Strategic Advisory Committee of the Idaho National Laboratory, the board of directors of Analytic Services, Inc., and other public and private-sector boards.

Appendix A Resource Adequacy, Cyber Contingency Response, and Power Restoration in an Inverter-Heavy Grid

Along with new dangers to reliability and security, inverter-based resources (IBRs) and distributed energy resources (DERs) create ways to strengthen grid resilience that were never before possible, including accelerated power restoration inside of blacked-out regions. The main report briefly highlights the opportunity to move from centralized blackstart cranking paths to highly dispersed, inverter-based restoration operations that could be much more difficult for the People's Republic of China (PRC) to target and disrupt. The first section of this appendix offers more detailed recommendations on such opportunities and on the underlying inverter technologies that both require and enable new approaches to grid resilience.

The transformation of the US generation fleet also creates perils beyond those examined in the main report. Most acute: the grid faces looming shortfalls in adequacy, which the North American Electric Reliability Corporation (NERC) defines as "the ability of the electricity system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements."[1]

IBRs and DERs are prime contributors to adequacy risks. NERC has determined that "new solar PV [photovoltaic], battery, and hybrid resources continue to flood interconnection queues, but completion rates are lagging behind the need for new generation." Moreover, "the performance of these replacement resources is more variable and weather-dependent than the generators they are replacing." Combined with surging demand for power and retirements of thermal generators (coal, oil, and gas), these IBR/DER problems confront much of the bulk power system (BPS) with "critical reliability challenges."[2]

Resource shortfalls already create problems for powering data centers that support defense planning and operations, especially by providing artificial intelligence (AI) services. The importance of these services to the Department of Defense (DOD) (and the US economy as a whole) is rapidly growing. So too is the amount of electricity they require, not only in Virginia's "Data Center Alley" but in every region of the United States. New IBR-based hybrid installations can help meet these requirements. But in many cases, nuclear power plants and gas-fired generators will offer the best sources of power for data centers, including for "behind-the-meter" projects that directly serve data centers (versus providing power to the broader grid on which data centers can rely).[3] Increases in *all* types of generation, together with the development of small modular reactors, advanced geothermal, and other new kinds of resources, will be needed to fill the emerging gap between national security loads and the power available to serve them.

Also at risk is the other foundation of grid reliability, and one that is tied still more tightly to US security: reliable operation. Reliable operation constitutes "operating the elements of the [Bulk-Power System]

[1] NERC, *Glossary*, 2; and NERC, *Reliability Terminology*. On the problems that IBR deployments and other systemic changes are creating for employing traditional adequacy metrics, see Bose et al., *Evolving Planning Criteria*.

[2] NERC, *2024 Long-Term Reliability Assessment*, 6.

[3] NERC defines behind-the-meter generation as "a generating unit or multiple generating units at a single location (regardless of ownership), of any nameplate size, on the customer's side of the retail meter that serve all or part of the customer's retail load with electric energy. All electrical equipment from and including the generation set up to the metering point is considered to be behind the meter" (NERC, *Distributed Energy Resources*, 1).

within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."[4] The nexus between reliable operation and national security is tight. If adversaries can create cascading failures across the system, they will be able to create catastrophic blackouts far more efficiently than by attacking BPS entities one by one.

To limit the spread and severity of disruptive events, NERC requires that balancing authorities (BAs) retain generation contingency reserves to help conduct balancing and other emergency operations.[5] Those mandates do not account for the danger that China will disrupt large numbers of generation and transmission assets. NERC and its partners are already rethinking their requirements for resources necessary to manage increasingly severe weather events. As their efforts go forward, they should also examine whether and how to establish cyber contingency reserves.

Creating such a reserve requirement would entail formidable challenges. We cannot get blood from a turnip: establishing a reserve for cyber incidents will depend on resolving broader shortfalls in resource adequacy. Advanced batteries have quick response capabilities for incident response. Expanded battery energy storage system (BESS) deployments, along with increased spinning services provided by conventional generators,[6] would be needed to provide the necessary resources. And, of course, the owners of those resources will have to be paid to keep them ready for use in an emergency versus selling their power to other customers. A deeper problem: determining how large a cyber contingency reserve is necessary, given the many other ways that BPS entities can respond to disruptive events (including emergency load shedding). This appendix proposes options to size such reserves and employ them in ways that support existing BPS plans for conservative operations and grid emergencies.

The final sections of the appendix examine additional risks and resilience opportunities created by the IBR/DER deployments and the grid decentralization they enable. As these deployments grow, they reduce the available fault currents on the grid and may ultimately compromise the effectiveness of existing grid protection systems that prevent damage to large power transformers and other difficult-to-replace assets.[7] The availability of adequate ramping will also be at risk in an inverter-heavy grid. Batteries offer unique capabilities to provide this essential reliability service (ERS) in a cyber contingency. Whether electric vehicle (EV) batteries can contribute to emergency ramping depends on a host of unresolved technical, policy, and even psychological factors.

[4] NERC, *Glossary*, 35; NERC, *Reliability Terminology*.

[5] Contingency reserve "is the provision of capacity deployed by the BA to respond to a balancing contingency event and other contingency requirements, such as Energy Emergency Alerts (EEAs) as specified in the associated NERC Reliability Standards" (NERC, *Reliability Guideline: Operating Reserve Management*, 3).

[6] Spinning reserve "includes generation synchronized to the system and fully available to serve load within the Disturbance Recovery Period following the contingency event or load fully removable from the system within the Disturbance Recovery Period following the contingency event deployable in 10 minutes." Natural gas turbines offer a widely used source spinning reserves (NERC, *Reliability Guideline: Operating Reserve Management*, 4).

[7] Tuladhar and Banerjee, *Impact of the Penetration of Inverter-Based Systems*.

Inverter Characteristics and Emerging Capabilities to Provide Essential Reliability Services

The inverters on which solar, wind, and battery energy storage system assets rely are electronic devices that convert direct current (DC) electricity, which is what solar panels generate, to alternating current (AC) electricity, which the electric grid uses.[8] Grid-connected wind generation assets typically require inverters as well.[9] BESS rely on bidirectional equipment that converts DC electricity from battery storage into AC electricity during discharge for use on the electric grid, and AC to DC during battery charging.[10]

While both IBRs and DERs rely on inverters, grid operators and regulators differentiate them in terms of where they are connected to the electric system. Under NERC's definition, IBRs are tied to the BPS—more specifically, connected at the BPS's transmission and sub-transmission levels.[11] FERC also defines IBRs as resources that provide power "to be transmitted on the bulk-power system."[12]

DERs, such as solar installations and BESS, also rely on inverters but are not connected to the BPS. Instead, as defined by FERC, "DERs are small-scale power generation or storage technologies (typically from 1 kW to 10,000 kW) that can provide an alternative to or an enhancement of the traditional electric power system" and are located "on an electric utility's distribution system, a subsystem of the utility's distribution system or behind a customer meter."[13]

Both IBRs and DER inverters face similar requirements for improved reliability, including to sustain the production of power when grid disturbances occur. Both confront similar threats of adversary misoperation as well. However, because these two categories of resources are regulated in very different ways to address reliability and security risks, this study follows the definitions established by FERC and NERC to distinguish inverter-dependent DERs from IBRs.

The grid's transformation also highlights the need to reassess the relationship between reliability and cyber resilience. For the BPS, NERC defines reliability as the operation of the system "within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."[14] Preventing such failures remains as crucial a national security imperative as ever. If the PRC or other adversaries seek to black out multiple US regions, it will

[8] DOE, "Solar Integration."

[9] IBRs include modern wind turbines, meaning type 3 and type 4 wind turbines (NERC, *Introduction to Inverter-Based Resources*, 2; and Forsyth, Tu, and Gilbert, "Small Wind Turbines").

[10] DOE, "Solar Power Electronic Devices."

[11] NERC, *Introduction to Inverter-Based Resources*, 2.

[12] FERC, "FERC Proposes IBR Standards."

[13] FERC also states that DERs include "demand response, energy efficiency, thermal storage or electric vehicles and their charging equipment" (FERC, "FERC Order No. 2222: Fact Sheet"). This study follows this component of FERC's definition of DERs. The National Association of Regulatory Utility Commissioners (NARUC) offers a similar definition: DERs "are devices or technologies that interface with the electricity system (i.e., consume, store, or inject power) at the distribution level, either by directly connecting to the distribution utility's wires or on an end-use customer's system. DERs include distribution-connected renewable resources, energy efficiency, energy storage, electric vehicles, and demand response" (Bieler et al., *Aggregated Distributed Energy Resources*, 6).

[14] NERC, *Glossary*, 35.

be far easier to do so if they can create cascading failures that spread across those regions versus having to disrupt large numbers of BPS entities individually.

Yet, while strengthening grid reliability directly contributes to cyber resilience, the definition of resilience entails additional requirements. The *National Security Memorandum on Critical Infrastructure Security and Resilience* defines resilience as "the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions."[15] The vulnerability of IBRs and DERs to supply chain exploits and "Living off the Land" (LotL) attacks creates new problems for achieving resilience, and also new technical solutions—especially for speeding the recovery of electric service.

Inverter Operations for Reliability and Power Restoration

IBRs and DER generation assets differ in fundamental ways from the hydropower, nuclear, coal, and natural gas resources on which the US electric system has long relied. These traditional generation assets are "synchronous" resources that convert mechanical energy into electric energy through electromagnetic induction. By virtue of the kinetic energy in their turbines and other large rotating components, these synchronous generation resources inherently resist changes in system frequency, providing time for other governor controls (when properly configured) to maintain supply and load balance. Similarly, synchronous generation resources inherently provide voltage support during voltage disturbances.[16]

Inverters enable solar, wind, and battery energy storage system assets to provide power to the grid in an entirely different manner. These resources are connected to the grid by power electronics and do not rely on electromagnetic induction from machinery that is directly synchronized to the BPS. Instead, inverters accomplish DC-to-AC conversion by rapidly switching the direction of a DC input back and forth, enabling a DC input to become an AC output.

Inverter-based solar and wind resources also differ from synchronous assets in the variability of their power output, which changes as a result of weather, time of day, and other factors. Nuclear, hydro, and fossil-based resources are much better suited to providing steady and always available power. That makes it easier for grid planers to measure their capacity and account for their contributions to resource adequacy. As the BPS increasingly relies on IBRs to meet future power requirements, NERC has determined that this "resource mix transformation is making traditional capacity-based adequacy criteria obsolete."[17] Moreover, as noted above, natural-gas-fired generators are highly dispatchable; in response to orders from grid operators, they can quickly ramp their power output up or down to help meet changes in demand and provide other ERS.[18]

This appendix examines how the shift from synchronous to inverter-based generation creates difficulties for ensuring resource adequacy and ERS, and how BESS (and supporting regulatory initiatives) can help

[15] White House, NSM-22.

[16] FERC, *Final Rule: Reliability Standards*, 112–113; DOE, *Solar Integration*; and FERC, *Explainer on the Inverter-Based Resources*. Section three of this appendix examines the implications of reduced conventional generation for operating reliability.

[17] NERC, *2024 Long-Term Reliability Assessment*, 11. Subsequent portions of this study examine options to update resource adequacy criteria to account for cyber contingency reserve requirements and other factors.

[18] NERC, *2024 Long-Term Reliability Assessment*, 8–10. The ability of gas generators to provide these services depends on the resilient flow of fuel to them. Winter storm Elliot and other severe weather events have disrupted these fuel supplies. So, too, could cyber-induced disruptions of gas transmission pipeline networks.

meet these challenges. Advanced inverter technologies can also derive novel resilience benefits from grid decentralization. Their greatest value may flow from their emerging capabilities to help accelerate power restoration in the aftermath of multiregional or nationwide blackouts, and—in the near term—maintain the stability of inverter-heavy electric systems when disturbances occur.

Grid-Following Versus Grid-Forming Inverters

To restart the grid after a wide-area blackout in the current US electric system, grid operators must first start up synchronous generators before they can connect IBR-generated power to the grid. The reason: when a large disturbance or outage occurs on the grid, conventional inverters will shut off power to these energy sources and wait for a signal from the rest of the grid that the disturbance has settled and it is safe to restart—known as "grid-following" (GFL).[19]

GFL inverters require an outside signal from the electric grid to determine when the switching will occur in order to produce a sine wave that can be injected into the power grid. In these systems, the power from the grid provides a signal that the inverter tries to match. The problem: with the retirement of older synchronous resources that generated this signal, and the growing deployments of GFL solar, wind, and battery resources, grid operators in inverter-heavy regions face growing difficulties in maintaining the stability of their systems.[20]

Grid-forming (GFM) inverters deployed on BESS provide the solution. GFM devices can generate the signal on which grid-following inverters depend and replicate the functionality provided by synchronous assets. NERC notes that "there are presently no universally agreed upon definitions of GFL and GFM inverter controls in the industry" but offers the following definition:

> Grid Forming Control for BPS-Connected Inverter-Based Resources are controls with the primary objective of maintaining an internal voltage phasor that is constant or nearly constant in the sub-transient to transient time frame. This allows the IBR to immediately respond to changes in the external system and maintain IBR control stability during challenging network conditions. The voltage phasor must be controlled to maintain synchronism with other devices in the grid and must also regulate active and reactive power appropriately to support the grid.[21]

In contrast to GFL assets, GFM assets most commonly use an instantaneously measured voltage signal rather than a processed signal from a phase-locked loop, as in a GFL inverter.[22] GFM response and support to the grid are instantaneous. NERC states that GFM technology has been recently proposed in the IBR industry for use in parallel with the bulk electric system, which, "when mature, is expected to address the majority of the risks and concerns of high (up to 100%) IBR penetration grid operation and stability with coordinated control and appropriate studies."[23]

---

[19] DOE, "Powering On with Grid-Forming Inverters."

[20] NERC, *Grid Forming Functional Specifications*, v–ix.

[21] NERC, *Grid Forming Technology*, iv.

[22] Current inverter-based generation sources generally use phase-locked loops, which rely on externally generated voltages by synchronous machines to operate.

[23] NERC, *Grid Forming Technology*, 9.

That process of maturation is well underway, and just in time. Surveying recent studies and findings from the operation of inverter-dominated systems in the Hawaiian Islands and elsewhere, NERC finds that such systems need GFM IBRs to maintain their stability. Two factors are making stability more practical to achieve. Not all inverters need GFM capabilities. NERC estimates that approximately 30 percent of inverters require such capabilities to keep an IBR/DER-heavy system stable, with the rest comprising cheaper (and widely deployed) GFL devices. Furthermore, new BESS can be equipped with GFM technology at "relatively low" incremental controller and hardware costs. Accordingly, NERC finds that "enabling GFM in all future BESS projects is a relatively low-cost solution that helps ensure system-wide stability," though further study is required quantify those costs and benefits.[24]

BPS entities are collaborating with manufacturers and other partners to set stability-focused functional specifications for batteries. For example, consensus is emerging that GFMs should provide autonomous, near-instantaneous frequency and voltage support by maintaining a nearly constant internal voltage phasor in the sub-transient time frame. NERC also recommends that GFMs be able to stably operate through and after the disconnection of the last synchronous machine in its portion of the power grid.[25] These performance features will be crucial to limit the impact of cyber disruptions on IBR-heavy electric systems and accelerate the restoration of power if major outages occur.

Operational, Communications, and Cybersecurity Considerations

An immense gap exists between developing GFM batteries that have technical capabilities to restart the grid and having the plans and capabilities to conduct restoration in the midst of a catastrophic blackout. The first step: ensure that GFM-equipped batteries earmarked for restoration actually have sufficient power stored for that purpose at all times. Doing so will require paying BESS owners to provide that service versus using battery capacity for day-to-day grid operations.

Conducting GFM-led restoration will also entail difficult operational problems. Once transmission system operators (TOPs) use BESS to establish initial power islands and begin energizing conventional generators to help grow those islands, they will need to carefully pick up load to keep those islands in balance, all amid the severe, multisector disruptions that a wide-area blackout would create. Load pickup via BESS will be especially complicated. Batteries cannot support as much inrush current as traditional synchronous generators of the same capacity.[26] These operational challenges will be all the greater if attackers disrupt the communications systems on which TOPs, reliability coordinators, and BAs depend to grow and integrate the power islands that GFM assets create.

Utilities and national laboratories are pursuing solutions to all of these problems. Led by the North American Transmission Forum (NATF), TOPs and their partners are developing "spare tire" communications capabilities to enable restoration even if adversaries disrupt both primary and backup control systems on which TOPs rely (i.e., total loss of energy management systems and supervisory control and data

[24] NERC, *Grid Forming Functional Specifications*, v. Appendix C examines the incremental costs of GFM versus GFL inverters in greater detail. For additional examples of GFM deployments in Australia, California, and Great Britain and the benefits of conducting additional demonstration projects, see Trabish, "Upgrading Inverters Is Urgent"; and Matevosyan, *Capturing the Reliability Benefits of Grid-Forming Batteries*.

[25] NERC, *Grid Forming Functional Specifications*, 1–2.

[26] DOE, *Battery Energy Storage Systems*, 18–19.

acquisition, or SCADA, systems). The National Renewable Energy Laboratory (NREL) is exploring how to manage inrush problems, enable multiple GFM inverters to collectively blackstart, and synchronize multiple microgrids for GFM-led restoration.[27] Advanced real-time modeling and simulation capabilities can help operators manage the complexities of power island formation and growth.[28] Industry standards are also emerging to help ensure that BESS will operate reliably, including IEEE 1547.3 for energy storage integration, UL 2941 for system safety, and SunSpec Modbus for communication protocols.[29]

No equivalent efforts are underway to require that security be built into GFM-capable BESS before they are deployed. The growing importance of BESS for grid stability and restoration will make GFM hardware, software, and firmware prime PRC targets. The main report emphasizes the importance of securing advanced IBR capabilities for frequency and voltage control from adversary misoperation. The same will be true of still more sophisticated GFM performance features, which—if accessed and manipulated by the PRC—could greatly extend the duration of power outages.

NERC's report on functional specifications for GFM BESS lacks any cybersecurity recommendations. Of course, NERC critical infrastructure protection (CIP) standards are broadly applicable to critical cyber assets and other potential BPS targets. But adversaries may employ attacks tailored to exploit BESS vulnerabilities, including via false data injection attacks and specialized threat vectors. Sandia National Laboratories finds that while "cybersecurity standards exist for adjacent systems" in the grid, "a research gap exists for specific policy for battery energy storage systems."[30] As NERC and its partners develop performance specifications for BESS, they should also create standards to prevent the misoperation of GFM capabilities and the widespread instabilities such attacks could create. The penultimate section of this appendix provides recommendations to do so.

Resource Adequacy: The Gap between Power Supplies and Future Demand

Efforts to derive security benefits from the US shift toward widely dispersed IBRs and DERs must grapple with a closely related problem: the danger that these resources (as well as conventional generation) will be unable to meet surging requirements for electricity, including from power-hungry data centers that provide essential AI services for national defense.

Two factors are putting adequacy and other measures of generation sufficiency at risk:

(1) *Demand*—the unanticipated and rapid growth of demand for power

(2) *Generation retirements and DER/IBR shortfalls*—the retirements of conventional generators, their slower-than-expected replacement by solar and wind resources, and the variable power output of those resources

[27] Sawant, Seo and Ding, *Resilient Inverter-Driven Black Start*; and Fix et al., *Multi-Microgrid Black Start Methods*.

[28] The use of real-time digital simulators (RTDS) offers an especially valuable tool to support islanding plans and capabilities (Wang et al., "Dominion's System Restoration Plan in RTDS"; and NATF, Spare Tire Approach).

[29] DOE, *Battery Energy Storage Systems*, 82.

[30] O'Brien, "Cybersecurity of Battery Energy Storage Systems."

Demand

The challenge of meeting rising requirements for power stems in part from our failure to predict them. Very little growth occurred over the past fifteen years. Efficiency gains in the use of electricity by appliances; heating, ventilation, and air conditioning (HVAC) systems; and other consumers of power helped limit power consumption even as the US economy expanded. The development of increasingly effective demand-side management (DSM) programs also helped incentivize customers to use electricity at off-peak times, thereby reducing pressure for expanded generation.

The days of marginal growth are gone. Based on load forecasts that utilities have provided to FERC, grid planners nearly doubled the five-year load growth forecast. The 2023 filings predict that nationwide electricity demand will grow from 2.6 to 4.7 percent over the next five years.[31] Other assessments project more dramatic growth over the long term. A September 2024 ICF analysis estimates that US-wide electricity demand will grow 9 percent by 2028 and 18 percent by 2033.[32]

These predictions understate the amount of generation resources needed to meet US power requirements. Grid managers need to meet not only total demand but also peak demand—that is, the maximum load on the electric system over the course of a day, month, season, or other specified period of time.[33] Episodes of extreme high and low temperatures spike demand when customers need power most for residential cooling and heating, and when the consequences of outages for public safety could be especially severe. NERC estimates that US summer peak demand will increase more than 122 gigawatts in the next decade, adding 15.7 percent to current system peaks, with winter peak demands increasing as well.[34] Meeting these spikes in power requirements will put pressure on efforts to ensure resource adequacy beyond those created by overall demand growth.

Within the overarching trend of rising electricity requirements, some states expect particularly steep increases. Georgia's main utility, Georgia Power, has boosted its demand projections sixteenfold.[35] Utilities in Virginia, Texas, and other states are predicting surges as well.[36] Furthermore, at the same time that loads are increasing, system operators must rely more on the variable output of solar and wind resources to help meet that demand. Gordon van Welie, president of ISO New England, testified to Congress on the combined effect of these developments:

[31] Wilson and Zimmerman, "Flat Power Demand Is Over."

[32] Chandramowli et al., *Power Surge*. A more recent study (Seiple, "Gridlock") predicts that US electricity demand will increase between 4 and 15 percent through 2029, with significant regional variations in that growth rate.

[33] FERC defines peak demand (used interchangeably with the term *peak load*) as "the maximum power requirement of a system at a given time, or the amount of power required to supply customers at times when need is greatest." The term "refers either to the load at a given moment (e.g., a specific time of day) or to average load over a given period of time (e.g., a specific day or hour of the day)" and is "usually expressed in megawatts" (FERC, *Glossary*). NERC offers a more detailed, BA-focused definition of peak demand, which is "1. The highest hourly integrated Net Energy For Load within a Balancing Authority Area occurring within a given period (e.g., day, month, season, or year). 2. The highest instantaneous demand within the Balancing Authority Area" (NERC, *Glossary*, 28).

[34] NERC, *2024 Long-Term Reliability Assessment*, 30–38; Walton, "'Explosive' Demand"; and Chandramowli et al., *Power Surge*, 6.

[35] Uberti, "Not Enough Power."

[36] Jankowski, "Demand from Large-Scale Users."

> We are transitioning to a power system that will have to meet a doubling of average demand and a tripling of winter peak demand by 2050. Moreover, this demand must be met with a resource mix where the majority of resources have variable production characteristics or are energy constrained under certain conditions. Our challenge is figuring out how much energy we will get from this evolving fleet of resources, how to ensure reliability through the wholesale market design and how to plan the transmission system to integrate the renewables and meet the forecast demand.[37]

Power Requirements for Data Centers and AI

The expansion of data centers, especially those providing AI services, is garnering headlines as the source of increased demand for power.[38] The Electric Power Research Institute (EPRI) estimates that data centers currently consume 4 percent of all US power generation. That demand could more than double to 9.1 percent by 2030.[39] Other studies anticipate still greater increases if the US economy continues to expand. McKinsey & Company, for example, projects that demand will grow from twenty-five gigawatts to more than eighty gigawatts in 2030.[40] Even these higher estimates may be overtaken by unexpected growth in data center/AI power requirements. In 2024, Exelon's "high probability" planned data load jumped from six gigawatts early in the year to eleven gigawatts in October, and other utilities are experiencing similarly greater-than-expected growth.[41]

The use of ChatGPT and other generative AI tools is accelerating these demand increases. EPRI has found that AI models are typically much more energy intensive than the data retrieval, streaming, and communications applications that drove data center growth over the past two decades. At 2.9 watt-hours per ChatGPT request, EPRI estimates that AI queries require ten times the electricity of traditional Google queries, which use about 0.3 watt-hours each; and emerging, computation-intensive capabilities such as image, audio, and video generation have no precedent.[42] The accelerating public and private-sector reliance on such advanced AI functions could produce explosive new power demands.[43]

Grid operators responsible for resource adequacy must also contend with regional variations in electricity requirements. In Northern Virginia's Data Center Alley, for example, utilities are already struggling to meet the demand for power created by data center expansion. PJM (the regional transmission operator, or RTO, for Virginia and much of the mid-Atlantic region) predicts that data centers will increase peak

---

[37] *Powering America's Economy, Security, and Our Way of Life* (statement of Gordon van Welie).

[38] This report employs the definition of AI provided by Exec. Order 14110 on AI and as set forth in 15 U.S.C. 9401(3): AI is "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action." The term *machine learning* means "a set of techniques that can be used to train AI algorithms to improve performance at a task based on data." In this appendix, machine learning is treated as a subcomponent of AI. Appendix B, which examines the use of AI for energy management and as a threat vector, differentiates between these two terms with respect to specific grid applications.

[39] Aljbour, Wilson, and Patel, *Powering Intelligence*, 2.

[40] Green et al., *AI's Hunger for Power*. For demand projections also greater than the EPRI estimate, see Seiple, "Gridlock," 3.

[41] Howland, "Load Has Nearly Doubled."

[42] Aljbour, Wilson, and Patel, *Powering Intelligence*, 2.

[43] Goldman Sachs, "Increase in Data Center Power Demand."

power demand for Dominion—the utility serving most of Virginia—by 50 percent over the next six years, with data center capacity growing by eleven gigawatts through 2030 and another ten gigawatts through 2040. That equates to adding more than the entire state of New Jersey's power demand to Virginia within a fifteen-year time span.[44]

Long-term developments could drive still greater increases in regional and nationwide data center/AI demand for electricity. At the furthest extreme, Leopold Aschenbrenner suggests that artificial general intelligence systems might ultimately become capable of researching, designing, and building better AI systems on their own. Aschenbrenner argues that such capabilities could accelerate US economic growth and offer significant benefits for planning and executing national security missions, but would also require vastly more power than current AI tools.[45]

Even without artificial general intelligence, the use of AI and other data center services is rapidly growing by the Department of Defense (DOD), the Intelligence Community (IC), and other federal departments responsible for US security. The electricity demand projections offered by EPRI and other organizations make no mention of these national security applications. That gap is understandable. DOD's *Annual Energy Performance, Resilience, and Readiness Report*, the authoritative document of DOD energy resource assessments, lacks any evaluation of AI demand among the hundreds of energy-related initiatives and appraisals mentioned.[46] As discussed in Appendix B of this report, DOD's uses of AI are expanding so quickly across warfighting and support missions that they are difficult to track, much less assess in terms of projecting the additional gigawatts in load they will create. One thing is certain: DOD will depend on the electric industry to serve these mission-critical loads at the same time that other power requirements are surging across the US economy.

Crypto, Manufacturing, and Much, Much More

Another new and rapidly expanding source of demand lies in cryptocurrency mining. The industry's total current power consumption is unknown. In 2024, crypto miners sued the US Energy Information Agency to discontinue gathering detailed information on power consumption[47]; the fate of future assessments is unclear. However, the demand is considerable. The agency's preliminary estimate suggests that electricity used for cryptocurrency mining likely represents between 0.6 and 2.3 percent of total US electricity consumption, including for bitcoin's power-intensive "proof of work" method of validating transactions.[48] Changes in federal policies, including the establishment of a US strategic bitcoin reserve, may drive a still greater increase in the industry's demands on generation resources.[49]

---

[44] Aurora Energy Research, "Data Center Demand."

[45] Aschenbrenner, "Situational Awareness." Section IIIa of Aschenbrenner's report examines artificial general intelligence power requirements, which constitute the "single biggest constraint" on the development and deployment of such systems. See also Toews, "AI That Can Invent AI."

[46] DOD, *Energy Performance, Resilience, and Readiness*.

[47] *Texas Blockchain Council v. Department of Energy*, Case No. 6:24-cv-99 (W.D. TX, filed Feb. 22, 2024); see 89 Fed. Reg. 18630 (Mar. 14, 2024) (withdrawing Notice of Information Collection).

[48] Walton, "Survey Bitcoin Miners about Electricity Consumption."

[49] Di Bartolomeo, "Trump's Top 3 Bitcoin Promises." Increased crypto mining demands on the grid in Texas and other crypto-heavy regions may also create problems for reliability, though the flexibility of mining loads may mitigate those risks. Peters, "Texas Leaders Worry."

Data center and crypto mining loads are only part of the broader increase in power requirements spurred by electrification across the US economy. While changes in federal and state policies concerning EVs could alter forecasts of their future electricity needs, these and other light vehicles already on the road consumed 7,596 gigawatt-hours in 2023, almost five times the consumption in 2018, and sharp demand increases are on track in 2024.[50] Building electrification is rapidly growing as well.[51] And if the electrification of manufacturing continues, especially for the production of steel, concrete, and other energy-intensive commodities, long-term demand could grow by hundreds of additional megawatts.[52]

In terms of grid decentralization and supply chain risk management, three types of increased manufacturing loads are especially significant:

(1) *Battery manufacturing*. Just six battery manufacturing plants were operating in the United States in 2021. A Wood Mackenzie study estimates that battery manufacturing capacity will rise twentyfold to 650 gigawatt-hours from 2020 to 2030, requiring 3,500 megawatts of new electricity demand.[53]

(2) *Solar manufacturing*. The Inflation Reduction Act of 2022 has drastically expanded proposed facilities for solar manufacturing. Before this act was passed, cells and wafers—the two components requiring the most energy when creating a solar panel—were not manufactured in the United States at all. The act has led to proposals for facilities that would produce forty-four gigawatts of wafers and seventy-five gigawatts of cells every year. While not all of these plants will ultimately be built, electricity demand from solar manufacturing is likely to rise by an estimated seven thousand megawatts.[54]

(3) *Computer chip manufacturing*. The digitization of equipment and control systems plays a crucial role in grid decentralization. Providing secure, domestically produced computer chips to support this transformation is vital as well. Two hundred billion dollars in private-sector spending is driving the construction of new or expanded US semiconductor fabrication facilities, with additional funding provided by the CHIPS and Science Act (CHIPS Act) and other government sources. There are no publicly available estimates of the total electricity demand this industry will create. However, a single fabrication plant being constructed by TSMC in Arizona could soon consume more than a gigawatt of electricity.[55] Multiplied by all other projects that are underway, US semiconductor manufacturing will create massive new power requirements.

The jump in demand needed to support the decentralized, inverter-heavy grid poses a quandary for resource adequacy. On the one hand, it is essential to escape from US dependence on Chinese products that undergird the grid's transformation, especially for batteries and other systems that are ripe for PRC disruption or misoperation. On the other hand, manufacturing domestic alternatives will heighten demand at a fraught moment for resource adequacy, when retirements of conventional generation resources in a growing number of US states are outpacing the deployment of IBRs/DERs necessary to (1) make up for the loss of those resources and (2) meet burgeoning demand for electricity.

[50] Ray and Brown, "Light-Duty Vehicles."

[51] Nadel, "Coming Electrification."

[52] Gimon, "Full Industrial Electrification."

[53] Seiple, "Gridlock," 6.

[54] Seiple, "Gridlock," 6.

[55] McGready, Post, and Nakano, "Energy Considerations."

Generation Retirements and Resource Adequacy Risk

John Moura, NERC's director of reliability assessments and planning analysis, aptly summarizes the predicament facing the United States: "our infrastructure is not being built fast enough to keep up with rising demand."[56]

Retirements of conventional generation contribute to this mismatch. Gas-fired power plants are the leading provider of conventional generation in most US regions, and their contributions to resource adequacy and operating reliability remain robust. In fact, on the record-setting day of August 2, 2024, these plants generated more than seven million megawatt-hours of electricity, making up almost half of all electricity generated in the contiguous United States that day (6.8 percent more than the previous summer's record set on July 28, 2023). The importance of gas-fired resources reflects their increasing use by grid operators to manage the intermittent output of wind and solar, as well as the overall increase in requirements for generation created by hotter weather.[57]

At the same time, however, some regions face a wave of coal- and older gas-fired plant closures. Generator owners and operators were on target to retire 5.2 gigawatts of US electric-generating capacity in 2024. The US Energy Information Administration expects natural gas to experience the most shutdowns in 2024, with the 2.4 gigawatts of scheduled retirements of natural gas capacity representing 46 percent of expected US capacity retirements in 2024 and 0.5 percent of currently operating US natural-gas-fired capacity.[58] Coal retirements, projected to increase to 10.9 gigawatts in 2025, are especially notable.[59] Many regional transmission organizations and independent system operators (ISOs) could face still more extensive fossil retirements and mismatches between the pace of those closures and the rate at which they will be replaced with solar and wind resources.

That replacement rate is lagging requirements for resource adequacy. NERC notes that "new solar PV, battery, and hybrid resources continue to flood interconnection queues, but completion rates are lagging behind the need for new generation." Moreover, the performance of these replacement resources is more variable and weather dependent than the generators they are replacing. As a result, less overall capacity (dispatchable capacity in particular) is being added to the system than what was projected and needed to meet future demand."[60]

PJM again exemplifies these challenges. Its market monitor, Monitoring Analytics, determined that about twenty-four to fifty-eight gigawatts of thermal resources—or 12 to 30 percent of the PJM Interconnection's installed capacity—is at risk of retiring by 2030 without a clear source of replacement generation. Furthermore, while renewables can replace a significant amount of the energy output of conventional resources, their variability results in comparatively less capacity. The result, according to PJM's market monitor: "The

[56] Walton, "'Explosive' Demand."

[57] "Low natural gas prices, the addition of new combined-cycle generating capacity, and increased generator capacity factors" also contribute to this heavy reliance on gas-fired plants (Wheaton and Ricker, "New Daily Records").

[58] S&P Global, "Lowest in 16 Years."

[59] Ray, "Retirements."

[60] NERC, *2024 Long-Term Reliability Assessment*, 6, 8.

simple fact is that the sources of new capacity that could fully replace the retiring capacity have not been clearly identified."[61]

PJM itself is closely examining these risks. The company's research reveals trends that, taken together, "present increasing reliability risks during the transition" from current to future resources "due to a potential timing mismatch between resource retirements, load growth and the pace of new generation entry under a possible 'low new entry' scenario."[62] PJM cites the following key trends:

- The growth rate of electricity demand is likely to continue to increase from electrification coupled with the proliferation of high-demand data centers in the region.
- Thermal generators are retiring at a rapid pace due to government and private sector policies as well as economics.
- Retirements are at risk of outpacing the construction of new resources, due to a combination of industry forces, including siting and supply chain, whose long-term impacts are not fully known.
- PJM's interconnection queue is composed primarily of intermittent and limited-duration resources. Given the operating characteristics of these resources, we need multiple megawatts of these resources to replace 1 MW of thermal generation.[63]

In subsequent review of these trends, PJM found that increasing demand poses an even greater challenge to resource adequacy than previously assessed. Driven by "end-use electrification, electric vehicles and data centers . . . recent history of this growth has proven unprecedented and dynamic. Average growth estimates for PJM's summer peak, for example, have increased by 375% between the 2022 and 2024 load forecasts—from 0.4% per year to 1.6% per year. This trend adds to the complexity of ensuring reliability through the energy transition."[64]

Other US regions are experiencing similar threats to resource adequacy as load growth accelerates and generation shifts from conventional to IBR resources. In the Southwest and other areas with high IBR penetration, the intermittence of solar and wind power creates serious problems for resource adequacy at times of peak load. In the far West, the Western Electricity Coordinating Council (WECC) concludes that if nothing is done to mitigate the IBR-related risks to resource adequacy within the Western Interconnection, "by 2025 we anticipate severe risks to the reliability and security of the interconnection."[65] The Midcontinent Independent System Operator (MISO) area and other regions are also at "high risk" of incurring shortfalls in their reserve margins—the additional generation resources that grid operators must have available to deal with contingencies.[66]

---

[61] "PJM has about 196 GW of installed capacity. It expects to process about 7.2 GW in projects that are in its interconnection queue by mid-2025 and 230 GW—mainly renewable generation—over the next three years, Jeff Shields, a spokesperson for the grid operator, told Utility Dive in late February" (Howland, "Up to 58 GW Faces Retirement").

[62] PJM, *Energy Transition in PJM*, 1.

[63] PJM, *Energy Transition in PJM*, 1.

[64] PJM, *Energy Transition in PJM*, 4.

[65] WECC, *Western Assessment of Resource Adequacy*, 4.

[66] Quotes are from NERC, *2023 Long-Term Reliability Assessment*, 7; more recent and even more severe assessments are provided in the *2024 Long-Term Reliability Assessment*. Reserve margin is defined as (capacity minus demand), where *capacity* is the expected

Severe heat and cold spells will drive peak demands still higher. NERC noted in its *2023 Long-Term Reliability Assessment* that the "wide-area, long-duration extreme weather events" occurring across multiple US regions can spike demand for heating or cooling while simultaneously disrupting power availability from IBR and conventional generation.[67] These manifestations of climate change put additional stress on resource adequacy. The *2024 Long-Term Reliability Assessment* issued a still more dire warning "that most of the North American BPS faces mounting resource adequacy challenges over the next 10 years as surging demand growth continues and thermal generators announce plans for retirement."[68] But natural hazards pale in comparison with the nationwide consequences of PRC attacks, which will require additional contingency reserves and contributions from BESS.

Reliable Operation and Contingency Reserves for National Security

BAs and other BPS entities have long focused on the need to maintain an adequate operating reserve to respond to contingencies. NERC defines operating reserve as "that capability above firm system demand required to provide for regulation, load forecasting error, equipment forced and scheduled outages and local area protection. It consists of spinning and non-spinning reserve."[69] From a grid security perspective, the most important category of such reserves is contingency reserves—"the provision of capacity deployed by the BA to respond to a balancing contingency event" or other emergencies.[70] In turn, contingency events constitute serious disruptions created by the sudden loss of generation or transmission outages that cause unexpected imbalances between generation and load on BPS interconnections—including, potentially, disruptions created by cyberattacks or combined cyber–kinetic attacks.[71]

NERC standards require BAs to maintain contingency reserves to respond to disruptions and help rebalance generation and load. However, existing metrics to determine the adequacy of contingency reserves do not explicitly account for the risk of multiregional cyberattacks. Many BPS entities already have emergency plans that include potential orders to generation owners to initiate "maximum generation" to help manage cyber disruptions. Moreover, NERC and FERC are already calling for the development of supplemental adequacy-assessment criteria that account for especially severe weather events. FERC and NERC might build on these measures to establish supplemental requirements to maintain cyber contingency reserves, and thereby strengthen US preparedness against PRC attacks.

Whether and how they should do so is fraught with uncertainties. BAs and other BPS entities have multiple tools besides contingency reserves to manage cyber incidents, including load shedding. And while increased reserves would almost certainly be helpful against multiregional attacks, determining "how much is enough" would depend on threat assessments that lie far beyond the expertise of the electric industry. Even the US IC is unlikely to be able to provide FERC and NERC with more than a very rough estimate

maximum available supply and *demand* is expected peak demand (EIA, "Reserve Electric Generating Capacity"). NERC's standard *BAL-002-WECC-3* also requires BAs to maintain a minimum amount of contingency reserve. On potential MISO shortfalls in reserve margins, see NERC, *2022 Long-Term Reliability Assessment*, 5.

[67] NERC, *2023 Long-Term Reliability Assessment*.

[68] NERC, *2024 Long-Term Reliability Assessment*, 6.

[69] NERC, *Glossary*, 28.

[70] NERC, *Reliability Guideline: Operating Reserve Management*, 3.

[71] NERC, *Reliability Guideline: Operating Reserve Management*, 3.

of the disruptive effects of a PRC cyberattack. Furthermore, at a time when the adequacy of US resources is already facing intensifying pressures, requiring industry to find (much less fund) cyber contingency reserves would present yet another challenge.

Nevertheless, given the potential consequences of a PRC attack and the urgency of exploring new mitigation options, FERC and NERC should begin discussions with their industry and government partners to assess the potential value of establishing cyber reserves and identify practical ways to provide them. Utilizing BESS to help supply reserves offers one such opportunity.

That leaves the question of who should pay to keep BESS and generation resources on tap for cyber incidents. Existing cost recovery mechanisms for investments in grid defense for BPS and distribution utilities provide a starting point for that discussion. Appendix C proposes a rule of thumb to allocate costs of defending the grid: investments that directly benefit national security, as opposed to broader improvements in reliable service, should be borne by the federal government versus ratepayers. Cyber contingency reserves offer a prime opportunity to apply that principle.

Emergency Operations and Cyber Contingencies

BAL-002-3—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event mandates that BAs or other responsible entities "make preparations to have Contingency Reserve equal to, or greater than the Responsible Entity's Most Severe Single Contingency available for maintaining system reliability."[72] Those entities are also responsible for determining what constitutes their most severe single contingency (MSSC). A BA might typically define its MSCC as the loss of its largest single generation plant or most critical transmission system component.[73]

A PRC attack could strike multiple generator and transmission targets within each BA's territory, creating a far larger loss of resource output than those authorities use to determine their contingency reserve requirements. BAs have often helped manage large-scale disruptions created by natural hazards by transferring power from neighboring authorities. However, in a coordinated, nationwide attack on the BPS, all sixty-six BAs in the United States might find themselves facing events more severe than their individual MSCCs, rendering power transfers impractical—especially if adversaries disrupt the tie lines and other transmission infrastructure that enables such transfers between BA regions.

NERC's critical infrastructure protection standards help BPS entities mitigate the potential severity of such events. In addition, FERC Order No. 893 provides incentive-based rate treatment to encourage voluntary investments in advanced cybersecurity technologies and utility participation in threat information–sharing programs.[74] Especially important: BAs and their BPS partners have robust plans for emergency actions and "conservative operations" to employ response measures, rather than relying only on the ability to rapidly increase (or, as needed, decrease) generation output. These additional response options and the

[72] NERC, *BAL-002-3*, 2.

[73] NERC's definition of MSCCs provides only general guidance as to what might constitute such an event: an MSCC is a single contingency "that would result in the greatest loss (measured in megawatt (MW) of resource output . . .to meet firm demand and export obligation (excluding export obligation for which contingency reserve obligations are being met by the sink BA)" (NERC, *Reliability Guideline: Operating Reserve Management*, 3).

[74] FERC, *Incentives for Advanced Cybersecurity Investment*.

emergency plans they support provide a foundation to assess the need for additional reserves and to effectively employ them when attacks occur.

Demand Reductions for Incident Response

PJM's *Emergency Operations* plan typifies the preparedness of BPS entities to coordinate on both demand- and supply-side actions "to prevent further propagation" of instabilities, including those caused by natural hazards as well as cyber and physical attacks. To employ demand measures, PJM can order transmission owners and distribution providers who participate in its market and balancing operations to request voluntary customer energy conservation or load curtailment and implement manual load-shedding.[75] Recognizing the value of such measures to manage grid instabilities, FERC Order No. 693 required that NERC's *BAL-002-2* allow BAs to use DSM as a resource for contingency reserves, and NERC has expanded its definition of contingency reserves to explicitly include capacity associated with DSM.[76]

With the growth of large-scale controllable loads across much of the United States, opportunities are emerging to expand the use of demand reduction to manage disruptive events. For example, the Electric Reliability Council of Texas (ERCOT) contracts with crypto mining facilities and other large customers to curtail their service in an emergency and then pay those customers when curtailments occur.[77] However, as noted in the main report, new security measures are essential to prevent adversaries from manipulating controllable loads to create (rather than limit) grid instabilities.

Involuntary load shedding provides an additional demand-side option for extreme events. NERC requires that when BAs and transmission operators are "operating with insufficient generation or transmission capacity," they "must have the capability and authority to shed load rather than risk an uncontrolled failure of the Interconnection."[78] In especially severe disturbances, transmission owners and distribution providers must to be able to conduct automated underfrequency load shedding "to arrest declining frequency, assist recovery of frequency following underfrequency events and provide last resort system preservation measures."[79]

Microgrid deployments and advances in facility in emergency power for critical facilities can mitigate the impact of automated load shedding on public safety and national defense. Nevertheless, sustained rotating blackouts or other deep, repeated service curtailments could help the PRC achieve its goals of inducing societal panic and impeding US crisis decision-making. Contingency reserves will continue to be a vital tool to supplement DSM and other emergency measures, especially against coordinated strikes that far exceed the individual and aggregate MSCCs of BAs nationwide.

---

[75] PJM, *Emergency Operations*, 14.

[76] NERC, *BAL-002-2 Background Document*, 6. BAL-002-2 has since been superseded by *BAL-002-3—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. However, under that updated standard, BAs can continue to use DSM as part of their contingency reserve.

[77] ERCOT, "Voluntary Curtailment Program." For the controversial use of these contracts by crypto mining facilities, see Sigalos and Smith, "Texas Paid Bitcoin Miner."

[78] NERC, *Standard EOP-003-1*.

[79] NERC, *Standard PRC-006-2*. In addition, NERC *BAL-003-2* requires BAs to have sufficient frequency response to maintain interconnection frequency within predefined bounds by arresting frequency deviations and supporting frequency until the frequency is restored to its scheduled value.

Supply-Side Emergency Operations

Under PJM's emergency plan, the organization can direct generation owners to increase output to maximum generation or reduce output to emergency minimum generation—whichever is needed to respond to grid instabilities.[80] These plans will need to evolve with changes in the grid and the loads it serves. For example, with large data center loads coming online, requirements may emerge to increase downward ramping if such loads are tripped because of faults or PRC attacks.[81] But with increasing pressure on resource adequacy, the principal challenge will lie in developing and executing realistic plans to ramp up generation.

When very rapid increases in power output have been required to restore the grid's balance in past events, two types of reserves have proven especially useful:

(1) *Operating reserve—spinning.* This type of resource includes generation synchronized to the system that is fully available to serve load and can be deployed in ten minutes.[82] These "spinning reserves" constitute the unloaded portion of generators that are online already and can quickly increase their output to their maximum ratings to meet changes in demand.[83]

(2) *Operating reserve—supplemental.* This category includes generation (synchronized or capable of being synchronized to the system) that is fully available to serve load within the disturbance recovery period after the contingency event or load that is fully removable from the system within the disturbance recovery period after the contingency event and can be removed from the system within ten minutes.[84]

Gas-fired generators (and coal and hydro, where available) have traditionally provided most of these spinning and supplemental generation assets. As pressures on resource adequacy intensify, grid managers, regulators, and ancillary service market operators will need to take special measures to ensure their availability. New opportunities are also emerging to boost and diversify the sources of contingency reserves. BESS are well suited to provide short-term grid contingency support within tens of seconds. Advanced BESS can also provide frequency regulation, ramping, and voltage support in a manner that can replicate current levels of ERS from synchronous resources.[85] Moreover, as long as we mitigate supply chain and LotL threats to BESS, the nationwide deployment of these contingency reserves will provide yet another way to leverage grid decentralization for national security.[86]

However, batteries can only provide contingency reserve functions if they are kept constantly charged and ready to perform in emergencies. Ensuring that battery owners and operators reserve them for contingency uses, rather than sell their power for other purposes, will require funding and incentives equivalent to those that ancillary service markets provide for conventional spinning reserves.

---

[80] These orders apply to generation owners controlling the output of a capacity resource (PJM, *Emergency Operations*, 13).

[81] NERC, *2024 Long-Term Reliability Assessment*, 38.

[82] NERC, *Reliability Guideline: Operating Reserve Management*, 4.

[83] EAC, *Optimizing Reserves*, 1.

[84] NERC, *Reliability Guideline: Operating Reserve Management*, 4.

[85] NERC, *Energy Storage*, 1–2.

[86] The final section of this appendix examines these BESS resilience issues in greater detail.

All such reserve sources could help limit the spread of instabilities in PRC cyberattacks. However, determining the additional requirements that cyber contingencies entail poses multiple challenges. The first lies in moving beyond existing adequacy metrics.

Setting Requirements for Cyber Contingency Reserves

Increasingly severe weather events and the rise of IBR/DER deployments are already creating problems for traditional criteria for resource adequacy and contingency reserves. NERC notes that current capacity-based adequacy criteria were not designed to differentiate between the scenarios, size, frequency, duration, and timing of energy shortfalls caused by severe weather events, as well as the rise of variable-output solar and wind resources.[87]

To account for these factors, NERC has called for the development of supplemental criteria to better assess system adequacy.[88] FERC has issued similar recommendations for updated metrics and measures to incentivize the provision of additional operating reserves, ramping products, and other ancillary services through the reform of markets for them.[89] In addition, NERC has proposed that BAs develop new energy emergency scenarios based on the "risks common" in their area that could compromise the availability of adequate resources, such as the disruption of natural gas supplies for multiple generating stations.[90]

These efforts are valuable but share a major limitation: none of them require BAs or other BPS entities to account for the danger of cyberattacks or the need for reserves to help counter them. Few BAs are likely to identify a PRC attack as a risk common in their areas, versus severe weather events or other disruptions to resource availability that they or their neighbors have already experienced. Building on the development of new metrics and scenario planning called for by FERC and NERC, these organizations and their industry and government partners should develop requirements for cyber contingency reserves. Doing so will raise an especially daunting problem: determining how much is enough in the context of emerging shortfalls in US resource adequacy.

Not only would setting cyber contingency requirements too high be impractical in terms of finding the necessary generation assets, but it could also create unintended reliability problems. In establishing current contingency reserve requirements, NERC argued that even though events larger than MSCCs do occur, requiring BAs to maintain and stay poised to use additional reserves could create risks to reliability. Even at MSCC levels, overly strict enforcement of reserve requirements could "have the unintended result of tying the operators' hands by removing the use of their available contingency reserve from their toolbox in order to maintain service to load or manage other reliability issues."[91] Mandates to raise contingency reserve requirements for cyber response should provide BAs and their partners with flexibility sufficient to meet more common reliability needs.

Such increases would also cost money. In the Southeast and US regions where vertically integrated utilities operate both generation and transmission systems, many of those utilities would need to contract for

[87] NERC, *2024 Long-Term Reliability Assessment*, 11.

[88] NERC, *2024 Long-Term Reliability Assessment*, 11, 21.

[89] FERC, *Reforms to Address Changing System Needs*, 4.

[90] NERC, *Proposed Reliability Standards BAL-007-1 and TOP-003-7*, 1, 6–7.

[91] NERC, *BAL-002-2 Background Document*, 12.

additional generation capacity to meet increased standards, paired with possible contracts to curtail loads for major customers. In the mid-Atlantic, Northeast, and other regions where RTOs and ISOs operate reserve markets for independent generation owners, utilities, and other participants, equivalent spending increases would be necessary for supplemental generation and demand management.[92] Either way, keeping additional reserves on tap for cyber incident response would require additional capacity and spending at the same time that overall demand for power is already putting resource adequacy at risk.

Taking a Rough Cut: Options for Industry–IC Collaboration

A virtue of MSCC-based standards is that they are relatively simple to calculate. Setting an equivalent basis to size reserves for cyber response operations is vastly more difficult. Indeed, the problems of doing so are so severe that it is tempting to preemptively declare defeat and abandon the whole notion of establishing cyber contingency reserves. But for the reasons discussed above, MSCC-based reserves are sure to fall short of need in multiregional PRC attacks.

The cost of supplementing existing reserve requirements will depend on the scale of instabilities that a PRC attack would create and, given the other emergency response measures available to BPS entities, how much reserve capacity will be needed to prevent the spread of instabilities across the three US interconnections. We cannot expect NERC, BAs, or other BPS entities to make such a determination on their own. Ideally, DOE and other components of the US IC will be able to provide a design basis threat to help the electricity subsector create an "MSCC on steroids" standard to assess the adequacy of contingency reserves for the emerging security environment.

Of course, the IC is unlikely to provide a precise assessment of the generation and transmission assets that the PRC will disrupt. A host of analytical uncertainties will impede the development of such fine-grained estimates, including the effectiveness of US grid defenses vis-à-vis the offensive capabilities that Beijing is holding in reserve for future crises. Nevertheless, even a general, broad-brush assessment would be better than leaving BPS entities in the dark on potential contingency requirements and hobbled in their ability to help protect service to critical defense and public safety loads.

Efforts to explore whether and how to establish cyber reserves could build on emerging efforts of FERC and NERC to assess requirements for responding to increasingly severe weather contingencies. NERC's *TPL-008-1—Transmission System Planning Performance Requirements for Extreme Temperature Events* requires transmission system planning coordinators to establish extreme heat benchmarks and "evaluate and document possible actions designed to reduce the likelihood or mitigate the consequences and adverse impacts of the event(s) if analyses conclude there could be instability, uncontrolled separation, or Cascading within an Interconnection."[93] BAs and their partners should consider whether these natural-hazard-focused actions (including increased transmission infrastructure and access to emergency generation capacity) might be adapted to simultaneously improve resilience against cyber and physical attacks, and thereby strengthen multi-hazard preparedness for little additional cost.

[92] For examples of how such markets function for contingency reserves and other ancillary services, see PJM, "Ancillary Services Market"; and ERCOT, *Ancillary Services*.

[93] NERC, *TPL-008-1*, 7.

FERC, NERC, and BPS entities should also explore whether to establish a specialized cyber contingency reserve guideline or standard, over and above the requirements of *BAL-002-3*. This option could leverage the likelihood that the United States will have strategic and tactical warning of an impending PRC attack, enabling grid managers to temporarily call up resources that would ordinarily be allocated to meet peacetime power requirements. Existing utility plans and capabilities for "conservative operations" and other emergency measures provide a foundation to help implement such a cyber-specific, on-warning approach.

Developing a Warning-Based Strategy to Identify and Employ Cyber Contingency Reserves

NERC's Standard *EOP-011-1*, *Emergency Operations*, requires transmission operators and BAs to develop operating plans to mitigate emergencies, including for generation redispatch and load shedding.[94] NERC also operates an alert system to disseminate "information that is critical to ensuring the reliability of the bulk power system."[95] Based on these and other standards and sources of data, RTOs, ISOs and other BPS entities maintain and exercise plans to transition to conservative operations when they receive warnings of severe natural hazards or elevated risks of cyber or physical attacks. MISO offers an example of this preparedness, stating:

> If conditions warrant, MISO will carefully transition from normal operating conditions to Conservative Operations to prepare local operating personnel for a potential event, and to prevent a situation or event from deteriorating. During conservative operations, non-critical maintenance of equipment is suspended or in some cases, returned to service. Operating personnel throughout the affected area are also in a higher state of alert. Conservative operation declarations may be initiated due to system conditions including severe weather, hot/cold weather, or geo-magnetic disturbance warning.[96]

PJM's plans go beyond natural hazards and explicitly recognize cyber and physical attacks as potential triggers for conservative operations, including strikes "that cause transmission outages, loss of generation, loss of load, damage to facilities." PJM also states that it could transition to conservative operations based on Department of Homeland Security (DHS) Homeland Security Threat advisories and other sources of federal intelligence.[97] DOE, DHS, and its partners should explicitly design such warnings to prompt BPS entities to immediately prepare for, and if necessary employ, cyber contingency reserves as part of their broader resilience measures against major adversity-induced instabilities.

Grid security emergency orders (GSEs) provide the best means to issue cyber contingency warnings. Under section 215A(a) of the Federal Power Act, the president has the authority to declare a GSE when there is an "occurrence or imminent danger" of cyberattacks, physical attacks, or other specified events against defense critical electric infrastructure (DCEI).[98] DCEI, in turn, constitutes any electric infrastructure located in any of the forty-eight contiguous states or the District of Columbia that serves "critical

[94] NERC, *EOP-011-1*.

[95] NERC, "About Alerts."

[96] MISO, *MISO Operating Procedures*, 1.

[97] PJM notes that such events could require the PJM RTO to operate "more conservatively (i.e., operate some margin away from the reactive transfer limit)" (PJM, *Emergency Operations*, 71).

[98] 16 U.S.C. § 824o–1, (a)(7). For a detailed analysis of GSEs and opportunities to preplan for their use see Stockton, *Resilience for Grid Security Emergencies*.

defense facilities" designated by the secretary of energy. Once the president declares a GSE, the secretary has the authority to issue orders for measures that "are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure during such emergency."[99]

Thus far, NERC, the Electricity Subsector Coordinating Council (ESCC), and DOE have focused on exercising the possible use of GSEs to prioritize the restoration of power to critical defense facilities.[100] These partners should expand future exercises to build preparedness for measures to protect the reliability of critical electric infrastructure when there is an imminent danger of cyberattacks, including measures to prepare for the use of cyber contingency reserves. As recommended in previous exercises, including the GridEx tabletop series, these partners should also preplan to consult on the content of such orders to maximize their effectiveness and avoid inadvertent risks to reliability.[101]

BPS managers should also pre-identify generation assets that could serve as cyber contingency reserves and (building on existing ancillary service markets and their ongoing expansion for sever weather events) contract with generation owners to provide such services in grid security emergencies.[102] As suggested in Appendix C, the federal government should reimburse BPS entities for the costs of such investments that are directly tied to national security priorities (versus general improvement in grid reliability that ratepayers typically fund).

But all such initiatives will depend on having a large enough generation fleet to meet national security requirements. Meeting those requirements will entail an additional challenge for resource adequacy: serving the AI data centers on which DOD increasingly depends to defeat the PRC and other potential adversaries.

Powering AI for National Defense

President Trump has declared that the United States must act decisively to retain leadership in AI and enhance US economic and national security.[103] Yet, DOE and electric industry projections of future demand do not yet account for the transformational role that AI will play in DOD warfighting and support missions and the need to compete against China's drive for AI supremacy. New opportunities are emerging to power AI for national security missions, including by colocating data centers with recommissioned nuclear power plants, new small modular reactors, and other resources. However, beyond such generation requirements, it will also be crucial to ensure that operators have adequate reserve margins to respond to cyber-induced disruptions. Getting off the knife's edge of resource adequacy will require much broader collaboration among industry, government, and regulators, starting with recognizing the importance of such adequacy for defending the nation.

[99] DOE, *Grid Security Emergency Orders*, 1174, 1177.

[100] NERC, *GridEx VI Lessons Learned Report*, 5–6, 10–11.

[101] NERC, *GridEx VI Lessons Learned Report*, 10–11.

[102] For an example of the expanded use of ancillary service markets for emergency reserves, see ERCOT, *Ancillary Services*. For a somewhat different approach to purchasing contingency reserves and other ancillary services, see PJM, "Ancillary Services Market."

[103] White House, *Trump Takes Action*.

AI-Enabled Warfighting and Implications for Resource Adequacy

AI-enabled systems can greatly improve the speed, quality, and accuracy of wartime decision-making. Yet, decision support constitutes only a small part of the Pentagon's turn toward these advanced (and power-hungry) capabilities. DOD's *Data, Analytics, and Artificial Intelligence Adoption Strategy* calls for a broad range of applications of these capabilities to "enhance the warfighting capabilities of the Joint Force," across the continuum "from the boardroom to the battlefield."[104]

DOD's increasing use of these capabilities constitutes a double-edged sword for grid resilience and overall US security. The department's reliance on AI and other data center services adds significant, unplanned-for requirements to the already explosive growth in civilian data center loads and in the economy-wide increase in electricity demand. These DOD requirements will intensify the challenges for resource adequacy created by generation retirements in the PJM service area and other data-center-heavy regions, exacerbating the difficulty of maintaining grid reliability and ensuring the availability of resources to respond to PRC-induced instabilities.

On the other hand, DOD's use of AI can also help prevent China from achieving the goals it would seek in striking the grid. As noted in the main report, the IC assesses that if Beijing feared that a major conflict with the United States were imminent, it might wage cyberattacks against US infrastructure to cripple the flow of forces to the region.[105] The US Indo-Pacific Command's Stormbreaker initiative exemplifies the potential value of AI tools to help adjust to such disruptions. Stormbreaker will use AI to facilitate planning, wargaming, analysis, and execution of multidomain, operational-level development of alternative courses of action. Army Maj. Gen. Joshua Rudd, Indo-Pacific Command chief of staff, said the initiative will greatly accelerate the process for developing courses of action, and will run that process "continuously, and red team it, war game it, simulate it over and over and over so that it's not only generating courses of action that you may not have thought about, but also refining the ones that exist."[106] These AI capabilities could help the command account for specific US transmission or distribution system outages and rapidly develop courses of action that maneuver around them to sustain force projection.

Other DOD applications of AI can directly support grid resilience if the capabilities are made available to utilities. Penetration testing is a strong candidate for such defense support. US Cyber Command (USCYBERCOM) and the National Security Agency (NSA) established a task force to test their AI implementation strategies and better inform the DOD's AI capabilities as a whole. As part of the task force's efforts, NSA is piloting automated, AI-enabled penetration testing designed to identify potential weaknesses in a network and enable users to see vulnerabilities through the eyes of the attacker. USCYBERCOM commander and NSA director Gen. Timothy Haugh states that this program "will provide a commercial solution for fully customizable AI-driven penetration testing to replace a previously manual process." Moreover, "once validated, we wanted to offer it as a full service" to industry via USCYBERCOM's cybersecurity collaboration center.[107] Such automated penetration testing could be enormously valuable for utilities, especially for smaller public power or rural cooperative systems that are crucial for supporting fort-to-port operations or other DOD missions.

[104] DOD, *Adoption Strategy*, 5.

[105] ODNI, *Annual Threat Assessment*, 11.

[106] Heckmann, "AI for Operational Planning."

[107] Welch, "CYBERCOM's New AI Task Force"; and USCYBERCOM, "AI Roadmap for Cyber Operations."

The most important benefit that utilities gain from DOD's exploitation of AI lies in "making the pain go away." Often used by utility leaders in private conversations, this phrase reflects their belief that DOD's most helpful role is to disrupt the ability of cyber adversaries to strike the grid and reduce the severity and duration of the attacks that utility personnel and their security contractors will have to counter. DOD's *Data, Analytics, and Artificial Intelligence Adoption Strategy* calls for the department to use AI to develop "fast, precise, and resilient kill chains" and undertake other initiatives to bolster its warfighting capabilities in all domains.[108] As those efforts go forward, they could have immense benefits for grid owners and operators. Utility regulators, federal policymakers, and state, local, tribal, and territorial officials should treat the provision of power for DOD AI as a crucial contributor to infrastructure resilience and US defense.

The first step to ensure that the grid will have adequate resources to serve critical security-related data center/AI loads is to estimate that demand growth and provide the data to NERC, RTOs/ISOs, and other BPS entities as they assess future resource adequacy and capacity requirements for load-serving entities. As noted in the introduction to this section, *no* predictions of AI load by DOE or the private sector account for the impact of AI power consumption to support national security missions. EPRI's 2024 report on powering intelligence typifies this failure to explicitly account for security-related requirements.[109] DOD itself falls short in assessing its AI loads from both commercial and government-owned facilities. The department's authoritative documentation of DOD energy requirements and resilience issues lacks any assessment of AI loads.[110] Nor do the detailed Government Accountability Office (GAO) critiques of DOD AI planning call attention to such gaps or propose how to fill them. Most notably, while a 2023 GAO report offers detailed recommendations on how DOD should manage the acquisition and support of AI services, it says not one word about power requirements.[111]

And while those loads are only part of the growth in AI's overall power requirements, treating security-focused AI as a lesser included case would be a mistake. Targeted investments in site-specific generation and in transmission/distribution infrastructure will be necessary to serve DOD and interagency data center loads, in addition to the grid-wide resources needed to power AI use by the defense industry and other widely distributed contributors to national security. Measures to ensure resource adequacy will also need to account for shifts in the location of these loads, including not only the concentration of AI providers in Data Center Alley but also the rise of modular data centers that support DOD operations in a highly distributed way.[112]

The assistant secretary of defense for energy, installations, and environment, or ASD(EI&E), should conduct such assessments of power requirements to serve DOD. ASD(EI&E) should also assess the location of those loads and share that data (with appropriate security protections) with generation and grid infrastructure owners and operators to help them meet defense data center power/AI requirements, and encourage the use of power purchase agreements and other established contracting mechanisms to fund the necessary generation. Other federal agencies should adopt a similar approach to meet their own security-related data

[108] DOD, *Adoption Strategy*.

[109] Aljbour, Wilson, and Patel, *Powering Intelligence*, 2.

[110] DOD, *Energy Performance, Resilience, and Readiness*.

[111] Ludwigson et al., *DOD Needs Department-Wide Guidance*.

[112] AWS Public Sector Blog Team, "Modular Data Center."

center/AI power requirements, with DOE integrating their assessments to share with NERC and other resource adequacy stakeholders.

Broader coordination among the National Security Council, the electric industry, and data center companies will also be necessary to shape policies and infrastructure investments to help achieve national security goals. With the help of DOE's new AI data center engagement team, the task force should collaborate with both providers and consumers of data center power to help meet their electric infrastructure support needs. And for federally owned data centers, departments should continue to use power purchase agreements and other traditional contracting vehicles to meet their electricity requirements.

Information on national-security-related loads must also be protected from PRC espionage and exploitation. Many TOPs and distribution providers already have robust measures in place to protect such information vis-à-vis the military bases they serve, thereby helping to impede planning and execution of supply- and demand-side attacks. These entities should apply the same measures to data centers.

Emerging Options to Power AI and Meet Overall Demand Growth

As the task force, the electricity subsector, data center hyperscalers, and other stakeholders grapple with specific ways to serve data center/AI loads, they can make progress on both the power supply and demand aspects of resource adequacy.[113] On the latter, significant opportunities are emerging to moderate the requirements for additional generation by making their operations more energy efficient. Shifting the times at which data centers draw power from the grid offers an immediate opportunity to achieve such efficiencies. For example, while AI model training demands a large amount of electricity compared with some other functions, data center operators can shift those training activities to periods of lower overall demand (and, potentially, lower electricity prices).

Advanced data center management systems can also schedule workloads to match peaks in solar and wind power production, thereby helping grid operators meet the broader challenges of balancing demand with variable IBR output. In addition, just as transmission systems can move electricity between regions to support balancing and efficiently serve peak loads, linking data centers with high-speed, high-capacity data transmission connections could allow them to move workloads seamlessly from one location to others where power is abundant.[114] EPRI is partnering with Meta and other hyperscalers to establish up to ten "flexibility hubs" that will develop innovative data center and power supplier strategies and explore how data centers can use power more efficiently and support balancing and other grid operations.[115] Innovations in cooling technologies, energy management systems, and other advances can also moderate data center power consumption.[116]

Yet, improvements in energy efficiency will never be sufficient to meet McKinsey's projection of a fifty-five-gigawatt increase in data center load between 2024 and 2030, with national security-related uses of

[113] Hyperscalers are companies such as Amazon Web Services (AWS) and Meta that operate large-scale data centers offering massive computing resources, typically in the form of an elastic cloud platform. Organizations use them to deploy and manage large-scale applications and services. Palmer, "Hyperscalers."

[114] Daniell, "Data Centers' Role."

[115] Walton, "Data Center Flexibility Initiative."

[116] DOE, "Cooling Control Systems."

AI rapidly adding to that total. Meeting these power requirements will necessitate that policymakers, regulators, and the electric industry boost supplies of electricity far beyond the rate at which it is growing today.

A Full-Spectrum Approach

No one type of generation alone will be sufficient to ensure resource adequacy for national security and the economy. For years to come, the United States will need an "all of the above" strategy to boost power production from IBRs, nuclear power plants, gas-fired generation, and other resources. We also need initiatives across a broad spectrum of opportunities to increase the availability of electricity where it is most needed.

DOE has provided a starting point to develop and implement such a full-spectrum strategy. *The Future of Resource Adequacy* identifies crucial areas for energy sector investments to increase available power:

- *Grid expansion.* "Expanding transmission capacity supports resource adequacy through enabling new generation and power transfer within and between regions. Transmission capacity is critical to facilitating the interconnection of energy generation in queues across the country."[117]
- *Balancing support.* Programs to shift the use of electricity to off-peak hours and otherwise shape energy usage can help operators balance supply and demand in ways that supplement other resource adequacy initiatives.
- *Expanding hybrid plants that combine variable energy production (especially solar and wind) with BESS.* "Hybrid arrangements help variable generators provide greater contributions to resource adequacy and can be deployed more rapidly than standalone storage systems when combined with existing generator resources."[118]
- *Long-duration energy storage (LDES).* DOE calls for the expansion of pumped storage hydropower and other systems with storage durations of ten or more hours, including (1) "inter-day LDES (i.e., power shifted by 10–36 hours)" and (2) "multi-day/week LDES (i.e., power shifted by 36–160 hours)."[119]
- *Grid enhancing technologies (GETs) and reconductoring.* The department notes that "using readily available, low-cost GETs to expand grid capacity can be much faster than building new transmission." Prime opportunities for applying these software and hardware technologies include dynamic line rating, advanced power flow control, and topology optimization. "Reconductoring existing transmission lines, particularly with higher capacity advanced conductors, can quickly expand grid capacity to interconnect new generation and improve resource adequacy."[120] A report by the GridWise Alliance identifies additional GTE-related options, including the use of advanced sensors and system automation tools, to increase the carrying capacity of existing transmission infrastructure.[121]

[117] DOE, *Future of Resource Adequacy*, 3.

[118] DOE, *Future of Resource Adequacy*, 15.

[119] DOE, *Future of Resource Adequacy*, 15.

[120] DOE, *Future of Resource Adequacy*, 21.

[121] GridWise Alliance, "Vision for an Integrated Grid."

DOE has also offered recommendations specifically focused on increasing the availability of power to data centers, including through the use of existing nuclear infrastructure to serve those loads.[122] But efforts to revive the Three Mile Island (TMI) nuclear plant exemplify the formidable regulatory and cost-allocation problems that such initiatives entail.

Three Mile Island: Just the Beginning?

In September 2024, Microsoft announced an agreement with Constellation Energy to purchase twenty years of power from Constellation Energy's TMI power plant in Pennsylvania. One of the plant's reactors suffered a partial meltdown in March 1979. TMI's undamaged reactor resumed operations in 1985 and provided power until it was shut down in 2019 and slated for decommissioning. Under the agreement with Microsoft, Constellation will refurbish and restart that reactor once the Nuclear Regulatory Commission approves it to do so (perhaps as soon as 2028) and will sell all of the electricity produced by the plant to Microsoft.[123]

The power from TMI (now renamed the Crane Clean Energy Center) would not be directly connected to Microsoft's data centers via a behind-the-meter construct. That electricity would flow into the high-voltage transmission system overseen by PJM and then on to the data centers via the grid's transmission and distribution systems. But as the purchaser of the zero-carbon energy, Microsoft will use it to erase (in its own internal climate policy ledgers) the emissions from burning gas or coal to produce electricity that currently flows into its data centers.[124]

Other efforts to restart nuclear plants are underway as well. In late 2023, an energy technology company, Holtec International, began formally seeking federal permission to restart the Palisades nuclear plant on the edge of Lake Michigan near Kalamazoo, Michigan. Palisades had shut down just a year earlier. NextEra Energy's Duane Arnold plant near Cedar Rapids, Iowa, which shut down in 2020, may also be brought back into service to power AI data centers.[125] Proposals are also in progress to construct new multi-power plants. However, as highlighted by Georgia Power's Plant Vogtle nuclear reactors, which came online in 2024 seven years late and at a cost of $35 billion (more than double the original $14 billion estimate), new plants will need to incorporate significant advances in design and construction to be affordable.[126]

Data center owners are seeking to deploy small modular reactors as a more cost-effective alternative. Google and Kairos Power announced an agreement to eventually build up to seven small modular reactors providing up to five hundred megawatts of power, with the first unit to come online in 2030. Amazon is collaborating with X-energy to bring more than five gigawatts of new power projects online across the United States by 2039, which would represent the largest commercial deployment target for small modular reactors announced to date. In addition, Amazon has signed a memorandum of understanding agreement with Dominion Energy to explore the development of a project near Dominion's existing North Anna nuclear power station in Louisa County, Virginia. The project could bring at least three hundred megawatts of power to the Virginia region, where Amazon Web Services is rapidly expanding its data center footprint.[127]

[122] DOE, *Clean Energy Resources*.

[123] Elliott, "Three Mile Island"; and Morehouse, "Deal with Microsoft."

[124] Portuondo, "Big Tech."

[125] Moss, "NextEra."

[126] Bright, "What's Next for Nuclear?"

[127] Chernicoff and Vincent, "Major Inroads."

Other types of generation will also be able to serve future data center loads, including IBRs. Meta has so far contracted energy from seventy-five solar projects and twenty-one wind projects, totaling more than twelve gigawatts of renewable energy procurement it has already announced. In addition, the company has agreed to purchase all energy output from ENGIE North America's 260-megawatt Sypert Branch solar project in Texas when it comes online in late 2025. The project is located in Milam County, Texas, and will supply power to a Meta data center ten miles away in Temple. Meta has also contracted with Sage Geosystems to purchase up to 150 megawatts of geothermal energy to power its data center growth.[128] A one-gigawatt hydrogen-powered hub is under development in Huston to help meet AI demand in the region.[129]

Many of these initiatives would colocate new generation resources with data centers, including through "behind-the-meter" power plants that are directly connected to the centers.[130] But colocation also raises contentious regulatory issues and carries immense consequences for overall resource adequacy and national security.

On November 1, 2024, FERC issued an order rejecting an amended interconnection service agreement that would have facilitated expanded power sales to a colocated Amazon data center from the Susquehanna nuclear power plant in Pennsylvania that is majority owned by Talen Energy. The amended agreement would have increased the behind-the-meter connection between the power plant and the colocated data center to 480 megawatts from 300 megawatts in the existing agreement.[131]

Speaking at a FERC technical conference on the colocation of large loads on the same day that the commission issued its order, FERC commissioner Mark Christie said colocation is a "gargantuan" issue that affects resource adequacy and fairness to consumers, because the proposed agreement would divert power from the Susquehanna plant away from the broader grid. Christie said that "if you're taking dispatchable resources—and when we talk nukes, we clearly are talking dispatchable resources—if you're taking them out of the supply stack, what does that do to resource adequacy?"[132]

FERC chair Willie Phillips dissented, arguing:

> Today's order also creates a national security risk. There is a clear, bipartisan consensus that maintaining U.S. leadership in Artificial Intelligence (AI) is necessary to maintaining our national security. Maintaining our nation's leadership in this "era-defining" technology will require a massive and unprecedented investment in the data centers necessary to develop and operate those AI models. And make no mistake: access to reliable electricity is the lifeblood of those data centers. I am deeply concerned that in failing to demonstrate regulatory leadership and flexibility we are putting at risk our country's pole position on this critically important issue. *That* is simply unacceptable.[133]

[128] DiGangi, "ENGIE Strikes Deal."

[129] Sayegh, "Billion-Dollar AI Gamble."

[130] Behind-the-meter energy systems (including generation, vehicle charging stations, and BESS) are systems that are located on the customer's side of the utility's service meter, versus front-of-the-meter systems, which are interconnected with distribution or transmission systems and are typically operated by utilities (Cory, "Behind-the-Meter Projects").

[131] FERC, *Order Rejecting Amendments*.

[132] FERC, *Transcript*, 11–12.

[133] FERC, *Order Rejecting Amendments*, dissenting opinion, 2.

The trade-offs between serving AI loads with dedicated resources (whether through colocation, power purchase agreements, or other means) versus serving grid-wide demand are intensified by the prospect of sharply rising electricity prices, reflected most vividly in capacity markets. RTOs and ISOs conduct capacity markets to help meet future electricity needs. Rather than paying power suppliers directly for the energy they produce, a capacity market pays a power plant or other resource for its ability to produce power should it be required.[134]

PJM announced on July 30, 2024, that capacity costs will soar to $14.7 billion for the 2025/2026 delivery year—the twelve-month period that starts June 1—up from $2.2 billion in the previous auction. Steve Lieberman, vice president of transmission and regulatory affairs for American Municipal Power, calls that "a mind boggling, staggeringly incomprehensible number."[135]

Higher capacity prices can incentivize the construction of new resources, not only for nuclear and IBR plants but also for fossil generation. US utilities and investors plan to add 133 new natural-gas-fired power plants to the nation's grid, according to S&P Global Market Intelligence data. Projections of further growth foresee an 18 percent increase in US natural-gas-fueled power generation between 2024 and 2035, based on data from 121 utility resource plans.[136]

Efforts to meet demand and maintain transmission reliability are even prompting the restart of obsolescent coal stations. For example, PJM is attempting to extend the life of the Brandon Shores and Herbert A. Wagner coal plants near Baltimore, Maryland, which were slated to close by June 2025.[137] Similar efforts are underway in other regions.[138] Nevertheless, both for serving defense critical data centers and meeting broader adequacy requirements, the United States faces a widening gap between projected resources and escalating demand.

Conclusion: National Security as Part of the Solution

NERC argues that the shift toward these IBRs should prompt BPS entities to change the way they assess and plan for resource adequacy. A NERC workshop report states that "substantial uncertainty has been introduced into planning the system with the addition of energy-constrained resources (inverter-based resources such as wind and solar, and, at times, other fuels such as natural gas) that are highly dependent on weather and environmental conditions." Accordingly, the report authors argue that "industry's methods of planning for resource adequacy need to change" in ways that better account for the risks to these resources.[139]

134 NERC, *Electricity Markets*.

135 Howland, "PJM's Record Capacity Prices."

136 S&P Global, "Gas-Fired Plants."

137 Olivio, "Drive to Old Power Source: Coal." The lack of local generation also helps spurt efforts to keep Brandon Shores and Wagner in service, especially in the near term (PJM, *Wagner and Brandon Shores Retirements*). The broader point, as noted by Steve Naumann (former Exelon Corporation vice president responsible for transmission and NERC policy) in a discussion with the author: "don't retire what you have until you have reliable replacements."

138 Halper, "Running Out of Power."

139 Bose et al., *Evolving Planning Criteria*, 1.

That effort should include assessments of cyber risks and the resilience benefits of investments in resource adequacy. The capacity of the electric system to power AI and maintain contingency reserves for cyber incident response is immensely valuable to US security. Quantifying the likelihood of such attacks is far more difficult than doing so for severe weather events; Chinese leaders' political decisions and many other difficult-to-assess factors will determine whether the PRC will strike the grid. Nevertheless, in parallel with efforts to assess the "costs avoided" by investing in cyber resilience, NERC, FERC, and their government partners should explicitly recognize the value of resource adequacy for national security and use that importance to help enable investments in adequacy that are essential to meet future demand.

Protection Systems for an IBR/DER-Heavy Grid

Protective relays play vital roles in safeguarding transformers and other grid equipment from damage—and employees from electrocution. When these relays detect a fault or abnormal operating conditions, including those that cyberattacks will create, they send the signal to quickly shut down any electrical equipment associated with the faulty or abnormally operating power system. As an NREL report puts it, protective relays essentially serve as the "brains that determine when the appropriate circuit breaker tripping action should take place."[140] Circuit breakers then disconnect the faulty element and physically isolate the electrical power system from short-circuit disturbances.

The ongoing retirement of conventional generators, which provide system inertia and are synchronized with the grid's frequency (and are therefore frequently termed *synchronous generators*), poses challenges to the effective functioning of protective relays and other protection systems. When faults occur, conventional generators inject large amounts of current that can easily be detected by protection devices. Relatively low-cost devices, such as circuit breakers or fuses, then disconnect the part of the grid with the fault.[141]

IBRs being deployed today do not have the same inherent ability as conventional generators to inject large amounts of fault current. IBRs produce less short-circuit current to trigger protective device responses. With the increasing deployment of IBRs/DERs and the corresponding retirement of conventional generators, this loss of fault current could jeopardize the availability of sufficient fault current capabilities and the effectiveness of protection systems that rely on them.[142]

NERC cites these risks as a key challenge for BPS reliability. With changing fault current magnitudes and characteristics in parts of the system with the most IBRs, these changes have "the potential to invalidate current protection system designs."[143] Implementing the ride-through requirements of IEEE Standard 1547-2018 makes these challenges all the greater. The resulting DER upgrades have the unintended side effect of defeating the widespread reliance on undervoltage tripping as the de facto method for distributed solar generation detection of faults on local distribution systems.[144]

---

[140] Keller and Kroposki, *Fault Characteristics*, 3.

[141] Using high-fault currents to recognize faults in power systems is known as overcurrent protection (Denholm and Kroposki, *Power Systems Protection*, 1).

[142] Denholm and Kroposki, *Power Systems Protection*, 1; and PJM, *Regional Planning*, 41.

[143] NERC, *2022 Long-Term Reliability Assessment*, 18. See also NERC, *Short-Circuit Modeling and System Strength*, iv.

[144] McDermott et al., *Protection of Distribution Circuits*.

DOE emphasizes that because grid IBRs and DERs provide substantially different fault currents, significant new risks will emerge to grid operations. Of greatest concern: "The aggregate contribution of many DER scattered throughout the distribution grid could reduce the fault current level sufficiently to desensitize traditional overcurrent relays, trigger overcurrent protection, trigger protection device maloperation, or alter fault detection."[145] These system failures could magnify the effects of voltage surges and instabilities created by adversary attacks—including those produced by the manipulation of IBR voltage control capabilities. Moreover, given the difficulty and length of time needed to replace large power transformers that weigh up to four hundred tons and are the size of a small house, malfunctioning of the relays and other devices that protect these assets from damage would disrupt grid operations in especially significant ways.

Development efforts are underway to enable IBRs to provide additional fault current and modify protection systems to effectively perform without the current levels that have previously been necessary. For example, digital protective relays, which can better adapt to characteristics of IBR-heavy electric systems, are now replacing older electromechanical protection relays. All such changes must also account for the integrated operations of multiple devices that contribute to protection, which include not only protective relays but also circuit breakers, substation battery systems, and transformers.[146]

But as with other facets of grid modernization, the digitization of protection systems creates opportunities to attack them. Adversaries are already seeking to exploit the cyber vulnerabilities of advanced protective relays. For example, CISA issued an advisory in July 2022 alerting grid operators to the vulnerabilities of Schneider Electric relays. The agency warned that successful exploitation of these vulnerabilities may cause a denial-of-service condition and "allow an attacker to gain full control of the relay," which "could result in loss of protection to your electrical network."[147] Attackers can also manipulate the trip settings of these protection devices in ways that leave some devices desensitized to faults in their protection area, leading to larger outages and noncleared faults.[148] All of these threat vectors can increase the destructive effects of combined protection system–IBR attacks.

Utilities' growing reliance on remote access to protection settings and related controls magnifies the risks of adversary access and exploitation. NERC notes that operators can now "manage specified controls from virtually anywhere and at a cost far lower than what would have been possible otherwise." Properly secured, tools to remotely access and alter settings for protection systems and other devices can offer an efficient means of making such adjustments at scale. However, NERC warns that employing such tools "can lead to protection system and control system misoperations" and "can initiate more frequent and/or more widespread outages."[149] Protection system misoperation encompasses a range of potentially serious failure modes, including both failure to trip (which can damage equipment) and unnecessary tripping (which can create and exacerbate outages).[150] Moreover, NERC has found that "resource mix changes that involve growth in inverter-based generation sources can also impact wide-area protection and increase the need to

[145] DOE, *Cybersecurity Considerations*, 24.

[146] Kahn, "Cooperation."

[147] CISA, "Alert Code ICSA-22-055-03."

[148] DOE, *Cybersecurity Considerations*, 25.

[149] NERC, *2023 State of Reliability Technical Assessment*, 56.

[150] NERC, *Glossary*, 18–19.

coordinate protection with the distribution system."[151] Assessing and managing risks of adversary-driven misoperation should be a priority for security initiatives as IBR-driven changes in protection systems accelerate.

Exploiting relays is only one way adversaries can pair manipulating IBR frequency and voltage support capabilities with other actions to disrupt the grid. Many others, including disrupting the communications links required to manage IBR power flows and misoperating DERMS, are examined later in this section. The challenge for regulators and their industry partners is to understand the complex effects that such combined attacks will create. A grid with increasing solar, wind, and battery energy storage system assets will behave in ways that are very different from today's electric system, due in part to the characteristics of IBR versus conventional generation and also the two-way power flows that are growing between distribution systems and BPSs. We can be sure that adversaries are modeling these new operational characteristics as well and will design their attacks to create mutually reinforcing failures between closely connected grid functions.

Ramping, Balancing, and Advanced Energy Storage

Ramping is an ERS that reflects the need for grid operators to maintain a constant balance between the demand for power (i.e., the total load from all consumers of electricity) and the available supply of power to serve it. Ramping is the upward or downward control of generation assets needed to maintain load–generation balance. The closely related attribute of flexibility constitutes the ability of those assets to turn on and off quickly and frequently in a single operating day, enabling grid operators to balance load and generation during periods when either or both are rapidly changing.

The growth of IBRs is creating serious problems for balancing. Hydropower- and fossil-fueled generators are well suited for ramping and rapidly responding to generation–load imbalances, in part because they are readily available when grid managers need them. Their availability is not perfect, however: in the case of natural-gas-fueled generators, severe winter storms (and, potentially, cyber or physical attacks) can disrupt the flow of fuel on which they depend. However, if adequate measures are taken to harden fuel flows and other natural gas operations and infrastructure against such disruptions, gas-fueled generation is a reliable source of power for balancing operations.

Fossil and hydro power plants are also highly dispatchable: in response to orders from grid managers, these assets can quickly raise or lower their power output to help balance generation with load.[152] Solar and wind generation assets lack these balancing attributes. The output from PV arrays and wind turbines in a given region will vary with weather conditions, the time of day, and other factors. IBRs also create other problems for balancing. Significant gaps exist between the daily peak production of solar power in a given region (around midday) and peak demand (in the late afternoon and evening as the sun sets), and there are major seasonal disparities between the availability of electricity supplied by variable renewable energy and

[151] NERC, *2023 State of Reliability Technical Assessment*, 56.

[152] Dispatchability is defined by the Argonne National Laboratory as "the ability of a power-producing facility to provide required amounts of power (at or below the facility's nameplate rating) on demand of the grid operator . . . regardless of the time of day or weather conditions" (ANL, *Glossary*). To increase the dispatchability of solar and wind power, BESS are being used and other initiatives are underway. See, for example, Price, *Dispatchable Solar Power Plant Project*.

total customer needs.[153] Moreover, while renewable energy resources can be dispatched down, they cannot be guaranteed to return to previous output levels or be dispatched up. Such "one-way" dispatchability will be utterly inadequate to conduct balancing during adversary attacks.

As long as robust gas generation capabilities exist, BAs can almost always dispatch enough generation to remedy looming supply–demand imbalances. Disruptions in generation can still jeopardize reliability, however. In February 2021, for example, winter storm Uri (which struck Texas and surrounding states) highlighted the risk of catastrophic multistate blackouts if gas pipelines and other infrastructure are not adequately weatherized.[154] NERC warns that severe weather events will continue to stress grid reliability and has recommended a series of measures for grid operators to build resilience against extreme cold and other events.[155] As long as gas generators provide large amounts of dispatchable, fast-ramping power, the intermittence of solar and wind power will pose only limited difficulties for keeping the grid in balance.

However, if IBRs continue to be increasingly deployed to help meet greater demand, they will need to gain ramping capabilities—just as they are acquiring capabilities for frequency and voltage support. Large-scale energy storage can help ensure that solar- and wind-provided power is available when needed for ramping. BESS in hybrid power plants and other facilities can also quickly ramp up or down to meet changes in demand. Over the longer term, batteries in tens of millions of EVs may be able to store and flow back power if the technical and operational challenges of such balancing can be overcome (and if EV owners agree to using them in this way). All of these initiatives, however, will create new attack opportunities.

Battery Energy Storage Systems

As discussed in the main report, BESS are undergoing a remarkable expansion. Total US battery energy storage capacity grew to 26.3 gigawatts, up from 16 gigawatts in 2023.[156] The US Energy Information Administration predicts that this rapid growth will continue into 2025 and beyond.[157] Moreover, NERC reports that requests are booming from BESS and hybrid power plant developers to interconnect their facilities with the BPS, making such grid-scale storage increasingly important for mitigating the intermittence of solar and wind power.

More traditional forms of energy storage have long contributed to the grid's management. Pumped hydroelectric storage is especially well established. Motors pump water uphill from a river or a reservoir to a higher reservoir; when the water is released downhill, it spins a turbine, generating power when needed. Pumped-hydro facilities serve as the equivalent of giant, permanent batteries, which are charged when water is pumped uphill and discharged as it flows down. New forms of pumped hydro are under development. They pipe water deep underground, and the pressure of the earth then squeezes the stored water back up to drive generators.[158]

---

153 Lawson, *Variable Renewable Energy*.

154 FERC, *February 2021 Cold Weather Outages*.

155 NERC, *Cold Weather Preparations*.

156 Jennifer L,"U.S. Battery Storage Hits a New Record"; and Antonio and Mey, "Capacity Expected to Nearly Double in 2024."

157 Ray, "U.S. Battery Storage Capacity Will Increase."

158 Hutson, "Renewable Storage," 4.

In addition to pumped hydro storage, a wide range of other technologies is creating additional opportunities for storage:

- *Mechanical energy storage.* Mechanical systems can store kinetic or gravitational energy for later transformation into electric power.
- *Hydrogen energy storage.* Hydrogen energy storage involves the separation of hydrogen from some precursor material, such as water or natural gas, and the use of that stored hydrogen to produce electricity from fuel cells or combined-cycle power plants.
- *Thermal energy storage.* In this form of storage, materials are heated or cooled so that their energy can later be recovered to produce power. Concentrated solar plants use molten salt as thermal storage medium and steam turbines to convert heat to electric energy.
- *Compressed air energy storage.* Compressed air storage contains energy in the form of pressurized air in a geological feature or other facility, with the pressurized air subsequently heated and used to drive turbines.
- *Supercapacitors.* Supercapacitors are high-power electrostatic devices with fast charging and discharging capability and low energy density. They have low maintenance costs, long lifetimes, and high efficiency.[159] These advantages are driving the rapid, large-scale deployment of supercapacitors across the US grid.[160]

However, while development and deployment of these and other advanced technologies are accelerating, a number of factors make BESS the preeminent means of storing solar- and wind-generated power. Battery systems are well adapted to manage the intermittence of these power sources. Hybrid facilities that combine PV arrays with BESS can store energy during the day, when power production is high and electricity prices tend to be low, and then discharge that power in the evening, when solar supply falls but pricing and demand for electricity are higher.

BESS expansion also reflects steep reductions in battery prices. Lithium-ion batteries lie at the heart of most such systems. Thanks to technological innovations and improved manufacturing capabilities, prices for lithium-ion batteries declined by over 70 percent from 2010 to 2016, and prices are projected to fall further.[161] Lithium supply chain problems and production constraints will make it increasingly difficult to meet total demand for such batteries, including from EVs.[162] However, the Bipartisan Infrastructure Law appropriated $7 billion to boost US battery production, and alternatives to lithium-ion technologies are becoming available for grid-scale applications, including lead-acid, redox flow, and (as noted above) molten salt.[163] DOE-funded initiatives are also spurring the development of LDES options that can store energy for more than ten hours at a time, far beyond the four-hour limit of many existing batteries.[164]

[159] The description of these storage options is drawn from NERC, *Performance, Modeling, and Simulations*, 3–4.

[160] Fortune Business Insights, *U.S. Supercapacitor Market*.

[161] Bowen, Chernyakhovskiy, and Denholm, *Battery Storage*, 1.

[162] McFarland, "Battery Shortage."

[163] For an overview of such spending initiatives and related DOE-supported battery research and development initiatives, see DOE, "Biden Administration, DOE to Invest."

[164] DOE, "Biden Administration Launches."

Financial incentives and regulatory factors provide a further impetus to BESS expansion. Colocating solar arrays and batteries can make the latter eligible for federal tax credits.[165] California, New York, Connecticut, and a growing number of other states have set aggressive energy storage targets, with some—including Virginia—requiring that their investor-owned utilities seek approval to reach specific storage goals.[166] FERC Order No. 841 integrates stored energy into the wholesale electricity market, thereby creating new opportunities for BESS operators to sell their power.[167] As conventional generation is replaced by IBRs, the ability of BESS to help balance the grid will further encourage investments in their expansion and create novel, digitally controlled balancing, ramping, and dispatch capabilities.

BESS Capabilities for Dispatch and Beyond

Thanks to the inverters and other power electronics on which batteries rely, BESS can replicate (and even improve) the ramping services provided by conventional generation. Those capabilities will help mitigate the reliability threats that growing solar and wind penetration would otherwise create. Advanced electronics can also enable BESS to provide frequency support and voltage control services that will be vital for responding to cyber-induced disturbances. However, batteries' dependence on inverters opens them to many of the same cyber vulnerabilities as IBR generation assets, including adversary manipulation. And as EVs provide massive, widely distributed storage opportunities for the grid, new risks of exploitation and wide-area instabilities will emerge.

The mix of BESS benefits and dangers reflects the central role that inverters play in their operation. Batteries convert stored chemical energy to DC electrical energy and vice versa. Inverters then convert that power to AC for delivery to the power grid and also manage the reverse process for batteries that can be charged up with power from the grid (as in the case of EVs).[168] Additional power electronics and control networks (including hybrid plant controls) manage the two-way power flows between these batteries and the BPS or distribution systems to which they are connected, on timescales that range from microseconds to tens of seconds to minutes.[169]

BESS electronic controls enable them to provide near-instantaneous power for ramping. These controls also enable battery systems to meet peak system demands for power, instead of relying on gas turbines and other types of peaking generation. BESS can enable energy time shifting as well, by storing low-value energy during periods of low demand and discharging that power during periods of higher demand. In addition, large-scale storage can provide operating reserves to help grid operators rapidly respond to disparities in supply and demand. Those reserves could be especially useful for responding to adversary-induced imbalances.[170]

---

[165] Gorman and Seel, *Batteries Included*.

[166] Plautz, "Policy Maneuvering Becomes Key." For examples of state storage targets and mandates, see State of New Jersey, *2019 New Jersey Master Plan*, 28; and Mai, "Maryland Passes Energy Storage Pilot Program."

[167] Hutson, "Renewable Storage," 5.

[168] NERC, *Performance, Modeling, and Simulations*, 3.

[169] NERC, *Performance, Modeling, and Simulations*, 3.

[170] Blair et al., *Storage Futures Study*, 7.

The advanced inverters and power electronics that control BESS also enable those assets to provide dynamic voltage support and frequency regulation (especially fast frequency response), operation in low short-circuit strength conditions, and other features that benefit grid reliability.[171] NERC recommends that the functions enabled by these new technologies "should be fully utilized (as needed) and are essential reliability services . . . for the BPS."[172] Combined with the deployment of IEEE 1547-compliant inverters for solar and wind generation, the wide distribution of such advanced storage systems could enable the development of new strategies to protect the flow of power to critical loads in a decarbonizing, centralized grid—if these IBRs can themselves survive attack.

Cyber Resilience Priorities for BESS

As with solar- and wind-based IBRs/DERs, the ability of battery storage systems to help manage grid balancing, frequency, and voltage creates opportunities for adversary mismanagement. Rapidly raising and lowering the discharge of multi-megawatt BESS offers one such attack vector. Attackers may also exploit the smaller but vastly more numerous (and largely unsecured) batteries deployed in distribution systems, which are now being aggregated for connection to the BPS. Moreover, as efforts accelerate to employ EVs for two-way power flows to the grid, these and other new forms of storage will create vulnerabilities that vehicle manufacturers and their resilience partners have yet to fully understand.

The dichotomy between BPS and distribution-level cyber standards applies to BESS as well as other IBRs. For battery storage systems that are part of the BPS, including hybrid facilities, mandatory CIP cybersecurity standards apply to those systems. However, security mandates and guidelines specific to the potential threats posed by energy storage systems are limited. NERC's reliability guideline on *Performance, Modeling, and Simulations of BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants* (June 2023)[173] provides detailed recommendations on how BESS can best provide frequency support and other ERS to help meet the reliability challenges posed by high-IBR-penetration systems. However, cybersecurity issues for BESS were not within the study's scope. FERC's proposed rule on reliability standards to address inverter-based resources (December 2022)[174] is similarly limited and does not call for measures to strengthen energy storage security.

Pathways already exist to fill these gaps. In its response to FERC's proposed rule, NERC suggested that in addition to addressing the reliability-related issues of BESS and other IBRs, it would be useful to analyze growing attack surfaces they were creating "where potential coordinated attack on multiple DERs or DER aggregators can impact the BPS. This includes the potential impacts of threats to the BPS from attacks on DER directly as well as an attack on DER aggregators controlling aggregate IBR-DER."[175] NERC and its partners should go forward with such threat assessments in ways that account for the specific risks to balancing posed by large-scale manipulation of BPS-connected energy storage. Recommendations to mitigate these risks may also apply to hybrid plants and storage facilities that are parts of the BPS.

---

171 NERC, *Performance, Modeling, and Simulations*, viii.

172 NERC, *Performance, Modeling, and Simulations*, viii.

173 NERC, *Performance, Modeling, and Simulations*.

174 NERC, *Proposed Rule: Reliability Standards*.

175 NERC, *Joint Comments*, 34.

In addition, as IEEE refines its *Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems* (P1547.3), additional opportunities will emerge to counter the massive misoperation of battery-provided power.[176] BESS resilience stakeholders should tailor security recommendations to address the specific cyber risks reflected in the advanced (and potentially exploitable) battery capabilities and other features called for in IEEE Standard 2030.2.1-2029, *Guide for the Design, Operation, and Maintenance of Battery Energy Storage Systems, Both Stationary and Mobile, and Applications Integrated with Electric Power Systems*.[177]

As with all such voluntary guidelines, however, problems will persist in ensuring compliance. Those difficulties will be especially significant for battery security efforts that will need to include participants far beyond the usual participants in grid resilience. EV manufacturers, charging station designers, aggregators of their stored energy, and transportation system regulators are emerging as increasingly prominent examples of the wider and more complex web of resilience stakeholders, illustrating the need to develop narrowly targeted, mandatory standards to counter the catastrophic effects that China will seek to achieve.

EV-Provided Grid Storage: Potential Benefits and Risks for Reliability

The Trump administration's executive order on unleashing american energy eliminates many of the policies that had previously helped spur the deployment of EVs and their charging stations.[178] Nevertheless, at the state level, government agencies, utilities, and EV researchers are likely to continue exploring how EVs might provide energy storage to help grid operators conduct balancing operations and, potentially, provide frequency and voltage support to limit the impact of grid disturbances.

These vehicles were originally designed for one-way power flows; similar to cell phones, they would draw power from the electric grid as needed to remain charged. However, with advances in EV power electronics, charging station capabilities, and other infrastructure and control systems, EVs are now capable of bidirectional flows of electricity with the grid. Especially useful, EVs can charge up during periods of low demand for electricity (typically at night) and then send power to the grid when demand is high. Moreover, with the help of smart inverters, such vehicle-to-grid operations can now support grid reliability and can be structured to provide the equivalent of mobile, distribution-level BESS.[179]

Advances in EV battery technology will increase the total capacity of grid-connected storage these systems may provide. Further increases will result from initiatives to harvest batteries from vehicles that are no longer in service and employ their "end of vehicle life" storage capacity for grid support. In addition, DOE notes that with the utilization of smart inverters and other advanced power electronics, EV-provided energy storage could support voltage control and contribute to system frequency response.[180] All of these attributes could help grid operators not only support day-to-day grid reliability as variable wind and solar generation grows but also respond to instabilities caused by extreme weather events or adversary attacks.

[176] IEEE, IEEE P1547.3/D3.12.

[177] IEEE, IEEE 2030.2.1-2019.

[178] Exec. Order 14154, 1, 5.

[179] Choi, "Essential Grid-Scale Storage"; Mafazy, *Vehicle-to-Grid (V2G) Standards*, 4–5; and EAC, *Enhancing Grid Resilience*.

[180] EAC, *Enhancing Grid Resilience*, 3; and NERC, *Electric Vehicle Dynamic Charging Performance*, 8.

It is not at all clear, however, that EV storage will offer a net benefit for grid resilience. EVs constitute DERs under FERC's definition of the term, and they increasingly rely on smart inverters for charging operations.[181] Accordingly, these vehicles and their associated infrastructure share many of the systemic vulnerabilities that DOE ascribes to other distribution-level IBRs. But EVs and their charging operations also present novel problems for reliability and dangers for security.[182] A working group composed of EV organizations, NERC, and other grid reliability stakeholders found that the "effects of grid dynamics, controls, and system stability due to the power electronic behavior of the EV charging loads may create new risks of widespread, cascading blackouts." Their research also determined that when grid disturbances originate from the BPS, EV charging behavior could exacerbate the resulting disruptions to the electric system and may result in "catastrophic consequences for grid reliability if left unchecked."[183] Adversaries seeking to magnify the effects of their attacks on the BPS could find these EV charging effects useful indeed.

In addition, attackers can directly target EV charging operations by accessing their internet-connected controls and creating large-scale disruptive shifts in power flows. This connectivity provides a wide range of opportunities for intentional misoperation of charging behavior, including via cloud-based communications, mobile application controls, and other means of simultaneously exploiting large numbers of stations and storage assets. IEEE warns that integrating EV infrastructures into legacy communication networks and protocols can help adversaries access and manipulate battery state-of-charging, load control, and other power flow features.[184] Adversaries can also use EV-related communications and control networks to feed false information to grid operators, thereby seeking to create system instabilities.[185] Finally, because EV charging entails loads that are connected to the grid through power conversion inverters, all of the attack surfaces that are endemic to internet-connected inverters will apply to the flow of EV-provided power.

NERC, NARUC, and other grid reliability stakeholders are intensifying their collaborative efforts with EV producers, battery providers, and charging station manufacturers to address such risks. Yet, extensive vulnerabilities are already being embedded into EV grid operations. For example, charging stations are typically controlled via communications with other parties without a third-party firewall or other cybersecurity devices to act as a shield; those protections must be built into the charging station itself. However, the complexity and rapid adoption of EV charging stations and technologies are leaving them vulnerable to attack.[186] These vulnerabilities are magnified by the nonstandard cyber–physical interfaces that typify today's EVs and charging stations.[187]

Risk mitigation efforts must also account for the attack opportunities created by the rapid build-out of the communications that control bidirectional power flows between EVs, charging stations, and the grid. Such networks are essential to authorize charging, sequence the charging process, and manage load (grid operators, vehicles, original equipment manufacturers, charging network operators, etc.). A Sandia National Laboratories report notes that "there is an incomplete industry understanding of the attack surface,

[181] Accelerate Group and EPIC, *Transportation Electrification Workstream*, 4, 19.

[182] NYU, "Shock to the System"; Johnson et al., "Electric Vehicle Charger"; and Lauver, "Cybersecurity Considerations."

[183] NERC, *Electric Vehicle Dynamic Charging Performance*, 5, 1.

[184] Alcade et al., *Integrating Cyber and Physical Security*, 104.

[185] Campbell, *Evolving Electric Power Systems and Cybersecurity*.

[186] Nawy, "Hackers Are Waiting."

[187] Acharya et al., "Cybersecurity of Smart Electric Vehicle Charging."

interconnected assets, and unsecured interfaces."[188] The authors examined some attack models involving malicious control of EV sharing infrastructure. However, they emphasized that other vulnerabilities have yet to be identified. The report also notes that sustained hardening measures will be necessary to counter emerging threats, including development of perimeter defenses to protect EV supply equipment and new intrusion detection and prevention systems.[189]

Cybersecurity standards for EVs and related infrastructure (including communication networks that can manipulate power flows with the grid) will be essential to drive the adoption of such protection measures. In June 2023, the American National Standards Institute, which administers and coordinates the US voluntary standards and conformity assessment system, issued its *Roadmap of Standards and Codes for Electric Vehicles at Scale*. It argues that because large-scale, coordinated attacks on charging infrastructure can produce blackouts over large geographical areas, it is essential to assess current and emerging gaps in EV-related cybersecurity. The report also notes that "the vast cross-sectoral nature of the EV ecosystem, combined with the complexity of systems and technologies required to integrate EVs onto the grid, exposes a multitude of cybersecurity risks."[190]

The roadmap offers two especially valuable recommendations to manage these challenges. First, "it is crucial to implement a risk-based approach that prioritizes addressing the most significant threats rather than attempting to cover all possible risks." The report cites firmware and software updates for EV charging stations as a potential high-consequence security gap that merits special attention.[191] Another risk-based option would be to focus security measures on extreme fast-charging infrastructure (e.g., four hundred kilowatts at one thousand-volt DC) and the vendor clouds that control them, since they increase the hazards and ability to impact the grid and vehicles more than lower-power charging systems.[192]

Second, the roadmap urges the establishment of a "broad, all-inclusive cybersecurity forum"[193] to identify and resolve security gaps in the EV charging ecosystem and, potentially, include codes and standards development activities. An initial step toward inclusive coordination across that ecosystem would be to strengthen the integration of standard-setting initiatives. IEEE 1547-2018 applies to EV equipment that interfaces with distribution systems, including requirements for grid support capabilities. Other standards organizations, including UL (formerly Underwriters Laboratories), the International Electrotechnical Commission (IEC), NIST, state PUCs, and SAE International, have their own guidelines and certification programs related to EV storage.[194] Forging unity of effort across these multiple (and potentially conflicting) public and private-sector initiatives will be essential for countering threats to the grid.

[188] Johnson et al., *Cybersecurity for Electric Vehicle Charging Infrastructure*, 3.

[189] Johnson et al., *Cybersecurity for Electric Vehicle Charging Infrastructure*, iii.

[190] ANSI EVSP, *Roadmap of Standards and Codes*, 153.

[191] ANSI EVSP, *Roadmap of Standards and Codes*, 153. The roadmap also calls for prioritizing efforts to create a multilayered defense strategy that combines technical, organizational, and procedural measures that would include initiatives for network segmentation, strong access control, encryption, and continuous monitoring; see also pp. 26 and 154.

[192] Sanghvi and Markel, "Electric Vehicle Fast-Charging."

[193] ANSI EVSP, *Roadmap of Standards and Codes*, 160.

[194] For a list of over two dozen initiatives completed or in process to establish standards, codes, and guidance documents for EVs and charging ecosystem, see ANSI EVSP, *Roadmap of Standards and Codes*, 161–164.

There are major impediments to strengthening such coordination. The relationship between NERC and the EV/charging community offers a case in point. Ryan Quint, NERC's former director for engineering and security integration, stated that he urgently wants to find the EV engineers to discuss risks and mitigation options, but "he doesn't know who to call. 'They're impossible to find,'" Quint reported.[195]

NERC established the Electric Vehicle Task Force in August 2024 to establish better connectivity and collaboration.[196] Other electricity organizations are seeking to do the same by leveraging their ties with EV and charging station manufacturers. For example, the EPRI's Electric Transportation Program has sustained dialogue between the electricity and EV industries for years.[197] NARUC and state PUCs have also been working with the EV community to develop load management strategies that can mitigate potential EV risks to the grid and maximize potential benefits.[198] Nevertheless, given NERC's responsibility for BPS reliability and security, and the rapidly intensifying threats posed by EV power flows, the lack of regulatory collaboration to counter these threats is astounding.

Gaps in coordination on EV risks also reflect a broader problem for securing the future grid. The shift from fossil-fueled vehicles to EVs is part of a multisector trend toward electrification that extends to manufacturing, building heating and cooling, and other economic activities and facilities. Data centers and other new large-scale consumers of electricity will further increase total demand for power. Accounting for all forms of electrification, Wood Mackenzie projects that by 2050 total electricity consumption in North America will increase by 66 percent.[199]

Moreover, as in the case of EV charging and "smart" buildings, many of these new power customers constitute loads that are controlled via the internet. Strategies to secure the grid must account not only for the nationwide deployment of vulnerable IBRs but also for new opportunities to manipulate the demand for power enabled by electrification, smart meters, and the Internet of Things (IoT).

[195] Ferris, "Needed: Car Experts."

[196] NERC, *Electric Vehicle Task Force*.

[197] EPRI, "Electric Transportation."

[198] Dixon et al., *Mini Guide on Transportation Electrification*, 2.

[199] Cited in NERC, *Electric Vehicle Dynamic Charging Performance*, 2. This projection is based on the expected increase in consumption of power by transportation and building electrification, after subtracting projected increases in on-site generation (e.g., rooftop solar PV).

Appendix B Employing (and Securing) Artificial Intelligence for Grid Resilience

The electric system is a hotbed of artificial intelligence (AI) innovation. In the last three years alone, over 695,000 AI patents have been filed and granted in the power industry, supporting the development of products for every dimension of grid planning and operations.[200] Some AI applications may seem far-fetched. Avangrid, for example, is piloting the use of robotic dogs to inspect substations.[201]

Nevertheless, three types of AI applications offer great potential to make the decentralized grid more reliable and secure:

(1) Tools that mitigate risks to resource adequacy through more efficient inverter-based resource (IBR)/ distributed energy resource (DER) utilization and planning

(2) Decision support tools for all-hazards resilience

(3) Capabilities to defeat AI-enabled attacks

The prerequisite to achieve these potential benefits: manage the risks of hallucinations and other AI errors and prevent adversaries from corrupting our AI tools and using them against us.

A dose of humility is needed in predicting how AI will alter grid operations. Many applications are in early stages of adoption, and little "real-world" data exists on the degree to which they actually succumb to AI failure modes.[202] Moreover, while some vendors may hype the value of their tools for controlling grid operations, the greater assessment risk may lie in the opposite direction: failing to foresee how improvements in computational power and AI systems will create astonishing grid control capabilities in only a few years.

To assess how AI tools will assist—or potentially replace—human decision-making, this study borrows from Department of Energy (DOE) nomenclature. AI can provide decision support to human operators (AI-assisted) with a human in the loop, or it can directly control infrastructure operations (AI-directed) with varying levels of human involvement (either supervised by a human on the loop or operating autonomously).

Owing to the potential consequences of AI mistakes, energy sector entities have indicated to DOE that active-control AI systems are less likely to be adopted in the near term than AI-assisted, human-in-the-loop decision support systems. Those consequences could include inadvertent blackouts that kill hospital patients or other victims and lead to wrongful death suits against utilities and their chief executive officers (CEOs). If utilities adopt direct control over their cyber defenses, the impact of AI failures could be vastly greater. Assumptions that AI tools cannot he held legally accountable for errors are constraining current research projects on automated control room operations.[203]

[200] GlobalData, "Who Are the Leaders in Electric Load Forecasting?"

[201] T&D World Staff, "Mobile Robot Dog."

[202] These potential sources of failure are examined in DOE, *Potential Benefits and Risks*.

[203] Choi et al., *eGridGPT*, v.

Yet, aggregators, virtual power plants (VPPs), and other distributed resource operators already rely on extensive AI decision support. With the continuing dispersal of DERs and IBRs, the growing complexity of power flows, the flood of data from phasor measurement units and other sensors, and improving AI capabilities, our dependence on AI will deepen and trend toward direct control in more and more facets of grid operations.

Efficient Inverter Resource Employment and Planning

Utilities employ AI every day to save money on routine, widely shared tasks. The use of AI applications for predictive maintenance is especially pervasive. These tools can assess sensor input on equipment status and performance and, with the help of specialized algorithms and historical datasets, identify and replace soon-to-fail parts with greater cost effectiveness than was previously possible.[204] Utilities are employing AI to develop rate cases, improve vegetation management, and carry out myriad other mundane but necessary functions.[205]

Other applications directly benefit the efficient employment of IBRs and DERs and thereby help close the emerging gap between available resources and growing demand. AI-driven improvements in weather forecasts, together with vast amounts of data on historical patterns, support the use of advanced modeling to predict and manage variations in solar and wind power production. These models also analyze predictions versus results over time to produce increasingly accurate projections.[206]

Utilities are now pairing AI output tools with ones that forecast electricity demand. Load forecasts analyze historical data, usage trends, and weather factors that influence electricity consumption to support short-term operational decisions involving DERs/IBRs and help assess future requirements for new generating capacity and transmission networks.[207]

Such AI-supported infrastructure planning is becoming increasingly valuable. The North American Electric Reliability Corporation (NERC) notes that "new solar PV [photovoltaic], battery, and hybrid resources continue to flood interconnection queues, but completion rates are lagging behind the need for new generation."[208] AI tools now help advance such projects through the siting, permitting, and interconnection process. The same is true of transmission expansion planning necessary to carry inverter-produced power to remote loads and dynamic-line-rating-based initiatives to increase the capacity of transmission lines based on weather and line conditions.[209] DOE, the Electric Power Research Institute (EPRI), and other organizations are developing still more advanced AI-enabled planning tools to speed the deployment and more efficiently utilize IBRs, DERs, and transmission infrastructure, and help mitigate the emerging risks to reliability and security posed by shortfalls in resource adequacy.[210]

[204] *Role of Artificial Intelligence* (statement of Jeremy Renshaw).

[205] Basrai, "Utility Rate Case Filings."

[206] *Role of Artificial Intelligence* (statement of Jeremy Renshaw); and T&D World Staff, "Energy Forecasting."

[207] GlobalData, "Who Are the Leaders in Electric Load Forecasting?"

[208] NERC, *2024 Long-Term Reliability Assessment*, 6.

[209] DiGangi, "The AI Paradox"; Mahdavi et al., "Transmission Expansion Planning"; Mansour Saatloo et al., "Dynamic Line Rating Forecasting"; and St. John, "Better Real-Time Data."

[210] DOE, "Operation and Planning Tools"; and EPRI, "Transmission Planning."

AI tools also support expanded DER deployments in an indirect but vital way by facilitating the sale of the power they generate. While Federal Energy Regulatory Commission (FERC) Order No. 2222 has enabled the growth of aggregator power sales to regional transmission organization (RTO) and independent system operator (ISO) electricity markets, the ability of distributed energy resources management systems (DERMS) and other software to meet local demand with locally produced energy is driving new ways of buying, selling, and valuating power in conjunction with balancing operations, including via the rise of transactive energy marketplaces.[211] DERMS-enabled economic dispatch constitutes another development. At any given moment, grid operators and asset managers strive to determine the optimal energy output needed to meet system load at the lowest possible cost. With widely dispersed solar and wind power, this optimization process is enormously complex and requires constant recalibration as weather and grid conditions change. AI tools now perform the same function automatically in real time to ensure reliable energy delivery at reduced cost.[212]

Decision Support for Dispersed Operations

A typical distribution grid control room system already monitors a million different network points in real time.[213] As distribution utilities deploy additional DERMS to meet escalating demand, along with advanced sensors and massive new data flows to monitor their systems and facilitate their control, the need to automate such functions will continue to grow.

The integration of power from aggregators and VPPs into distribution systems will create additional AI support requirements. Sandia National Laboratories found that human grid operators and asset managers already struggle to meet demand with the resources they directly control. Managing thousands of edge devices for bidirectional power flows—and many terabytes of real-time data—poses impossible challenges absent the use of AI tools and automated software controls.[214]

Yet, it is aggregators and VPPs themselves that are most heavily dependent on AI. Many VPPs combine AI-driven demand predictions and the ability to manipulate the power demand of end-use devices.[215] For example, AI-supported response programs can turn off or decrease consumption from DERs, such as smart thermostats, water heaters, and commercial and industrial equipment, when power supplies run short.[216] With AI tools, VPPs can also shift the timing of electric vehicle (EV) charging to avoid overloading local distribution system equipment, dispatch energy from EV batteries back to the grid, and perform specialized functions to maintain power quality.[217]

---

[211] Lowder and Xu, *Evolving U.S. Distribution System.*

[212] Veritone, "Artificial Intelligence Power Grids."

[213] Boyd, "Control Room."

[214] Larson, "DERMS;" and SNL, "Artificial Intelligence and Machine Learning."

[215] Demeo, "True AI-Driven Virtual Power Plants"; and Energies Media Staff, "AI-Driven Virtual Power Plants."

[216] Gupta, "AI in Demand Response."

[217] Sha, "Introducing VPPieces"; and Downing et al., *Virtual Power Plants*, 2. "Power quality is the measurement of how close to perfect an electrical voltage is at any given time or point. High quality electrical voltage is a sine wave that measures exactly what is expected in both voltage and frequency. A high quality electrical source is one that can deliver all the electrical energy needed without any change in the voltage" (PS&C, "Power Quality).

AI-enabled tools also help aggregators and VPPs manage DER-specific control problems. For example, these resources create overloads of power feeders and instabilities and can lead to the maloperation of legacy protection systems. The National Renewable Energy Laboratory (NREL) found that many distribution utility personnel are not adequately trained to cope with these issues. Advanced DERMS software and automated controls enable aggregators and VPP owners to make up for such shortfalls.[218] Researchers are also seeking to apply generative AI to help operators control DERs.[219]

In addition, AI tools help VPPs process increasingly large datasets generated by the deployment of connected and grid-interactive devices and advanced metering infrastructure, detecting loads in smart-meter data and facilitating the identification and enrollment of participants in VPP programs by providing customer segmentation. AI also facilitates (1) the coordination and dispatch of large multiasset fleets of devices; (2) automated balancing; and (3) the management of frequency or voltage disruptions on VPP systems.[220]

Bulk Power System Applications

The two-way flow of power between distribution systems and the bulk power system (BPS), combined with the widespread deployment of IBRs, advanced sensor networks, and digitally controlled devices, is driving BPS entities to adopt new AI-enabled decision support and automation tools. NERC notes that "with the progression of interconnected power generation, transmission, and distribution assets, the landscape of automated tools and systems has transformed. This evolution spans an array of digital information platforms and microprocessor-driven devices, fostering a technologically diverse environment wherein operators can wield unprecedented control from virtually any location at a fraction of the historical cost."[221]

While offering significant benefits for maintaining BPS reliability, the adoption of automated tools also creates new challenges. NERC states that "the proliferation of these systems introduces an increasing web of rules, algorithms, and interdependencies that amplify the intricacy of operation." Of special significance: "the swift decision-making capabilities of modern relays, tripping circuits, or initiating alternative actions within milliseconds epitomize the accelerated pace at which these systems must navigate intricate operational scenarios," especially in the context of expanding IBR deployments and the power management and coordination problems they entail.[222]

BPS entities are responding to these challenges by deploying increasingly powerful tools to support decision-making by control room personnel and further automate grid functions. Supervisory control and data acquisition (SCADA) systems and energy management systems offer especially important decision support tools. SCADA systems monitor and control the grid, whereas energy management systems provide advanced computations and visualizations of the system's current and contingent states. However, NREL researchers note that monitoring and measuring data is insufficient for effective grid control. It is crucial to transform this data into actionable information to enhance situational awareness for operators in

[218] Strezoski et al., "Integration," 277–279.

[219] Hansen, "GenAI"; and Wendel, "ChatGrid."

[220] Benes, Porterfield, and Yang, *AI for Energy*, 18.

[221] NERC, *2024 State of Reliability*, 39.

[222] NERC, *2024 State of Reliability*.

grid emergencies.[223] Maintaining situational awareness and employing grid data for incident management will be especially critical if the People's Republic of China (PRC) or other adversaries achieve wide-area disruptions that put the grid at risk of cascading failures.

Multiple initiatives are underway to help meet these resilience requirements by providing control room operators with new AI-enhanced decision support tools[224]:

- *Generative AI tools that analyze grid data and simulate scenarios with physics-based digital twins to provide response options for system operators to consider.*[225] By analyzing the context and parameters of an event, AI can also help operators identify the most relevant procedures and best practices to guide response operations. It can simulate scenarios and predict their outcomes to help decision-makers choose the most effective incident mitigation options.[226]
- *Model-based real-time analysis software*, as is now being employed by Pepco, that can detect abnormalities and coordinate voltage control.[227]
- *Tools that enable grid operators to use the massive amounts of data on the status of the grid provided by phasor measurement units.* These measurement units have been deployed at over twenty-five hundred locations across the nation's BPSs. They measure the magnitude and phase angle of electrical phasors in electric systems with great accuracy on a microsecond basis, which is much faster than the speed of existing SCADA technologies. They offer a potentially powerful tool for grid monitoring and incident response. At present, however, many utilities are overwhelmed by the flood of data these sensors provide and make only limited use of it for real-time grid management. AI tools can help address these challenges and support more effective response decision-making.[228]

AI tools to improve modeling and simulation are the next frontier. DOE and its national laboratories are exploring AI-enabled optimization models that simulate the electric system and the severity of disruptive events much more quickly than is possible with current widely used models.[229] National laboratories are also developing AI tools to help grid operators set a schedule for daily and hourly power generation to optimize power. Jeremy Renshaw, senior technical executive at EPRI, states that such optimization "is one of the most complex, computational problems in the world today." Indeed, "it is exponentially more complicated than even today's most powerful exascale computers can handle, especially for real-time optimization."[230]

Quantum computing may help meet this challenge and further our dependence on automated grid controls. A consortium of research organizations is exploring the use of quantum neural networks and quantum generative adversarial networks to predict when failures could occur in the energy grid and fix them

[223] Choi et al., *eGridGPT*.

[224] For an overview of these initiatives, see Behr, "Wanted."

[225] Choi et al., *eGridGPT*. For additional generative AI applications for controlling grid operations, see Choi, "Generative Artificial Intelligence for the Power Grid."

[226] Benes, Porterfield, and Yang, *AI for Energy*, 18–19.

[227] Dengler, "Faster-than-Real-Time Simulation."

[228] Yu, "Machine Learning Solutions."

[229] DOE, "Artificial Intelligence."

[230] *Role of Artificial Intelligence* (statement of Jeremy Renshaw).

prior to incident. Opportunities may also emerge to employ continuous variable optimization on quantum computers to balance distributed generation, future energy sources, and placement of equipment to increase grid resilience.[231]

All-Hazards Resilience and Cyber Defense

Many of the AI decision support and automation tools discussed above, including for managing frequency and voltage disturbances, will also be valuable to limit the spread of instabilities caused by severe weather, wildfires, or PRC attacks. Additional resilience-specific tools are also under rapid development and deployment.

AI is accelerating the development of capabilities for the grid to heal itself when disruptions occur. DOE states that "with its ability to rapidly ingest vast amounts of data and identify subtle shifts in data distributions, [AI] can be a powerful tool in creating 'self-healing' infrastructure, detecting and diagnosing anomalies, and improving situational awareness for operators to respond to various events."[232] AI products are under development to automatically reroute electricity around faults in milliseconds and restore power flows without human intervention.[233] Other emerging techniques enable autonomous detection and diagnosis of such faults and also further accelerate AI-led restoration operations.[234] Better still against cyberattacks: detect and counter them at machine speed so disruptions never occur or are far more manageable in scale.

Defeating Cyberattacks with AI: From Decision Support to Direct Control?

The 2021 report of the National Security Commission on Artificial Intelligence offers a vision that is less expansive but especially significant for the decentralized grid. The report finds that AI and machine learning have "current and potential applications across all the phases of cyber attack campaigns and will change the nature of cyber warfare" at an accelerating rate. In particular, the expanding application of existing AI cyber capabilities will make "cyber attacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyberweapons, and make cyber campaigns more effective on a larger scale."[235] Adversaries will seek to exploit all of these capabilities to undermine the potential security benefits of widely dispersed generation and localized grid control.

DOE highlights specific ways in which AI could soon help adversaries strengthen the effectiveness of their attacks against the US electric system. Improvements include:

- *Modeling the US grid.* Adversaries can use AI for model inference or model completion based on available data to help fill in missing details or information needed to design an attack on energy infrastructure. Adversaries with little to no information about a targeted energy system might be able to rely on the inference capabilities of AI tools to provide insights (whether factual or synthetic) that can inform attack design.

[231] QED•C, *QuEnergy*; and Di Giovanni, "Quantum Algorithms."

[232] Benes, Porterfield, and Yang, *AI for Energy*, 18.

[233] Dua, "'Self Healing' Tech Repairs Electric Grid."

[234] Kumar Maurya et al., "Self-Healing Grids"; and Pratt, "Rescuing the Grid."

[235] NSCAI, *Final Report*, 50–51.

- *Attack design.* AI tools can also be used to facilitate model-based design of attacks, allowing adversaries to combine AI inference with information about specific energy system infrastructure (aided by traditional modeling) to design and simulate more complex attacks that are optimized to create the most significant or disproportionate impact.
- *Adaptive attacks.* AI-driven autonomous malware may be able to flexibly adapt to the system it is attacking to more effectively seek out and target high-value systems within a network or autonomously make decisions to update its objectives over time.
- *Evasion of US defenses.* AI techniques can help cyberattacks escape detection by allowing attack tools to learn how to bypass firewalls, mask themselves from detection, or even masquerade as beneficial software—all of which would increase the difficulty of detection by defenders.
- *Mulimodal attacks.* AI can also enable autonomous control of devices for physical attacks. Adversaries could combine AI-enhanced capabilities with other technologies, such as uncrewed drone systems, to execute remote physical attacks on energy infrastructure.[236]

The speed of these AI-enabled attacks and the vast number of targets they could simultaneously strike will confront even the best-trained BPS security teams with immense challenges, much less aggregator, VPPs, and distribution systems attacked at scale. The AI commission emphasizes that "defending against AI-capable adversaries operating at machine speeds without employing AI is an invitation to disaster. Human operators will not be able to keep up with or defend against AI-enabled cyber or disinformation attacks, drone swarms, or missile attacks without the assistance of AI-enabled machines."[237]

Yet, cyber staffs are pretty well-off today compared to what lies ahead. As Richard Danzig notes:

> Processing speed and communication capabilities also increasingly tilt the equation against human decisionmakers, both generally and especially in military situations. Humans now proceed at about one-millionth the speed of machines. Machines are becoming faster. Humans aren't. When instant response is imperative, even our Defense Department's proponents of humans in the loop concede that their desired human control cannot be achieved. It can be anticipated that this exception will swallow the rule as the range of tasks that can be accomplished by machines grows, machine speeds increase (both in calculation and in kinetic operations), and autonomous operations proliferate.[238]

Humans are already out of the loop on many defense-related functions that would occur in a large-scale cyberattack. BPS entities have the ability to automatically disconnect large quantities of load in millisecond time frames to rapidly rebalance the power system and arrest frequency decline after a severe event. Grid circuit breakers and other protection system components function with equivalent "human-free" speed. Based on these and many other examples of autonomous operations, adopting additional AI-directed defense mechanisms would merely carry forward practices that are already ubiquitous.

The Department of Defense (DOD) policy on AI control of lethal weapons provides useful context for deciding how far to automate grid protection. The department states that "autonomous and semi-autonomous weapon systems will be designed to allow commanders and operators to exercise appropriate levels of

[236] DOE, *Potential Benefits and Risks*, 6.

[237] NSCAI, *Final Report*, 9.

[238] Danzig, *Technology Roulette*, 15.

human judgment over the use of force."[239] Grids rarely inflict casualties in the way that weapons do (squirrels excepted). However, as in the case of manual load shedding, decisions to cut off power to hospitals or prioritize the restoration of service to military bases instead of water systems could lead to significant loss of life. Few if any utility CEOs or their boards of directors would authorize AI tools to make such decisions without human input, especially if these leaders might be held liable for hallucination-driven AI mistakes.[240]

DOD's policy requiring appropriate levels of human judgment has a significant exception: the directive does not apply to "autonomous or semi-autonomous cyberspace capabilities."[241] Many of the tools that would be most valuable for AI-directed defense against cyberattacks fall into that category. Yet, beyond the imperatives for human control discussed above, additional factors make it useful to keep humans in (or at least over) the loop. For example, Danzig notes that humans can add "a different kind of reasoning to a system that relies on machines. . . . Machine systems can be hacked and misdirected in certain ways, while subversion of humans requires quite different tactics."[242] That additive reasoning could be valuable indeed in control rooms.

Grid operators should pursue a similar combined strategy to incorporate advances in both direct AI control and decision support tools. Automated threat detection systems (and third-party service providers to help operate them) have spread across the BPS. Such applications are vital to assist attack response decisions by human operators. When significant events occur, grid operators could receive hundreds or even thousands of notifications over a short time period. This phenomenon, known as an alarm cascade or swarm, can make it extremely difficult to determine the root cause of the failure and take appropriate action, especially if adversaries seek to avoid detection. A variety of new tools now exists to help distribution and BPS operators diagnose alarms and decide how to respond.[243]

The continued growth of DERs and IBRs and other assets will make these tools still more valuable. A DOE report states that "although identifying anomalies is straightforward in theory, the sheer volume of assets to monitor makes AI the preferred solution for ongoing detection and analysis."[244] The same is true for review of operational technology logs for cyber forensics, assessments of malware, and other activities supported by new AI tools, including an initiative by Southern California Edison (SCE) to enable DERs to continue operating while detecting or mitigating a cyber threat to achieve reliable, self-organizing monitoring and control during cyberattacks.[245]

The balance between reliance on direct AI control and decision support tools depends on the specific functions that help constitute grid defense as a whole. For example, utility and government leaders will always need to communicate with the public when cyber incidents occur and combat efforts by adversaries to leverage blackouts to incite social panic and influence US decision-making. We need to advance applications for both AI- and human-led defensive operations and combine their use in way that leverages their comparative advantages.

[239] DOD, *DOD Directive 3000.09*, 3.

[240] Pallardy, "New Forms of Liability."

[241] DOD, *DOD Directive 3000.09*, 3.

[242] Danzig, *Technology Roulette*, 13.

[243] Boyd, "Control Room."

[244] Benes, Porterfield, and Yang, *AI for Energy*, 19.

[245] DOE, "Nearly $23 Million."

Threats to AI and Mitigation Options

DOE usefully divides risks of employing AI into three categories: unintentional failure modes (including bias and extrapolation), adversarial attacks against AI, and compromises of AI software.[246] Multisector work is underway to reduce the danger of hallucinations, bias, and other sources of unintentional errors. To secure the AI tools on which US grid operators increasingly depend, some sector-specific risks and mitigation options deserve special focus:

- *Poisoning attacks* add, modify, or alter the data used to train an AI model in order to force the model to learn the wrong behavior. This can include modifying data on energy system operations so that a model develops an incorrect conception of what "normal operations" look like. It can also include more sophisticated efforts to create a "backdoor" that yields specific results when triggered—for example, poisoning the training data so that when presented with a specific image, a model meant to detect physical wear in oil and gas equipment never declares a piece of equipment to need maintenance.
- *Evasion attacks* use adversarial input data, which a human may find indistinguishable from regular data, to produce a desired model output—typically counter to the goals of the model creator. An evasion attack might alter the data presented to a model trained to predict energy market prices, doing so in a carefully engineered manner that causes the model to incorrectly overestimate or underestimate prices.
- *Data extraction* attacks seek to learn sensitive information about an AI model or the data it has been trained on. For AI tools that are customized for energy applications, or even tuned to specific energy infrastructure, a data extraction attack could allow an adversary to access the closely held information about an energy system of interest that is embedded in the AI tool.

Given AI systems' reliance on large datasets and algorithms, even small manipulations of these datasets or algorithms can lead to consequential changes in how the systems operate. The National Security Commission on Artificial Intelligence found that these threats are not hypothetical: adversarial attacks are happening and already impacting commercial machine learning systems.[247] A US Government Accountability Office report identified specific threat vectors that China could employ against grid control tools. The office found that "automated systems themselves are susceptible to a range of disruptive and deceptive tactics that might be difficult to anticipate or quickly identify. These threats are amplified by the ongoing delegation of decision-making, sensing, and authentication roles to potentially vulnerable automated systems. Moreover, broader deployment could become riskier as the reliance on autonomous decision-making increases."[248] All of these automated functions are coming to dominate aggregator and VPP DER operations.

The PRC is also developing new ways of reaching and manipulating AI tools, including both overt and covert specialized penetration of AI supply chains. For example, Chinese companies partner with major providers of AI tools to US customers. G42, an AI firm controlled by Sheikh Tahnoon bin Zayed of the United Emirates, is partnering with OpenAI, the creator of ChatGPT. G42's "stack," or its underlying technology infrastructure, has been built with the help of Chinese companies, including Huawei.[249]

[246] DOE, *Potential Benefits and Risks*, 4.

[247] NSCAI, *Final Report*, 52.

[248] GAO, *Information Environment*, 25.

[249] Mazzetti and Wong, "A.I. Giant's Ties to China."

The PRC can use such access to place physical backdoors on the chips they provide, creating holes in AI algorithms sold to US grid operators to enable system misoperation.[250] China can also seek to poison the datasets on which operational tools rely by maliciously manipulating the output of AI algorithms. In particular, a DOE report warns that "data poisoning or model poisoning involves corrupting the integrity of the dataset used in training to impact the AI model's ability to perform correctly (i.e., make correct predictions). By inserting artfully manipulated data, researchers have demonstrated the ability to generate incorrect and inaccurate results."[251]

However, much less artful penetration opportunities may pose the greatest risks. The State Grid Corporation of China has been the largest holder of new energy-sector AI patents from 2021 to 2023, with other Chinese companies making hundreds of patent filings as well.[252] As these patents help China sell advanced AI grid applications or subcomponents that find their way into US-provided tools, the dangers of supply chain exploits will grow.

Mitigation Measures

Although some best practices have been developed (if not consistently adopted), the highly distributed and digitized nature of VPPs will require the development of new security measures. DOE, in one of its *Pathways to Commercial Liftoff* reports, proposes a number of measures that VPP operators and their partners could pursue:

- Regulators, utilities, regional grid operators, and other VPP leaders could codify a set of accepted measures to minimize VPP performance risk within accepted and understood bounds.
- Research organizations, regulators, utilities, and regional grid operators could accelerate research, development, and adoption of distribution system reliability standards and requirements.
- Regulators, utilities, and VPP companies could incorporate and/or require common baseline cybersecurity measures and responsibilities that ensure that systems are secure by design and operated for resilience.[253]

All such initiatives that subsector partners *could* pursue are laudable. Many others that are not on the *Pathways* study's list of proposed actions would be helpful as well—starting with measures to prevent China from corrupting the AI models that aggregators, VPPs, and other power managers are rapidly deploying. But many of these efforts are in their infancy. Security recommendations that do exist are not being widely adopted by VPP owners/operators. And in the meantime, with DOE's support, VPP systems are growing nationwide in number, scale, and technical complexity. We are rapidly embedding AI applications across the grid to improve its efficiency and reliability. Policymakers, regulators, and industry must make the security of these applications a national priority as well.

[250] *Role of Artificial Intelligence* (statement of Paul M. Dabbar).

[251] Caddy et al., *Cybersecurity and Digital Components*, 11.

[252] GlobalData, "Who Are the Leaders in Power Generation Forecasting?"

[253] Downing et al., *Virtual Power Plants*, 45–47.

Appendix C Forging Unity of Effort across the US Electric System

As exemplified by the National Association of Regulatory Utility Commissioners (NARUC) cybersecurity baselines, distribution-level entities are taking aggressive measures to strengthen the security of distributed energy resources (DERs). Moving from voluntary compliance with these guidelines to consistent, mandatory security standards for DERs will entail significant challenges. The analysis below offers recommendations to support that transition.

A Reliability Construct for the New Threat Environment

Bulk power system (BPS) and distribution-level stakeholders differ in the ways they define and measure reliability. The North American Electric Reliability Corporation (NERC) definition of operating reliability for the BPS focuses on preventing cyberattacks or other disruptions from creating system instabilities, uncontrolled separation, or cascading failures.

Reliability is also a crucial goal for local distribution utilities regulated by state public utility commissions (PUCs). NARUC emphasizes that "State Commissions must ensure that the public have access to reliable service," and proposed utility investments to maintain the reliability of such service against emerging hazards (including severe weather and cyber threats) are the focus of many rate cases.[254] The National Rural Electric Association and the American Public Power Association are similarly dedicated to helping their members ensure reliable service.[255]

However, PUCs and their cooperative and public power counterparts typically assess distribution system resilience in ways that are unlike NERC's approach to operating reliability. That difference is rooted in the architecture of the two types of systems. The BPS is built around a tightly interconnected and synchronized set of high-voltage transmission systems and other BPS components. That structure puts a premium on preventing cascading failures and instabilities from spreading across the grid.

Local distribution utilities are not tied to each other in ways that make them vulnerable to equivalent cascading failures. Instead, regulators and utilities focus on assessing and improving the ability of individual distribution systems to provide reliable service to their customers, as measured by the customer Average Interruption Duration Index (CAIDI), the Customer Average Interruption Frequency Index (CAIFI), and related metrics.[256]

CAIDI and CAIFI remain valuable tools to assess the reliability of individual distribution utilities. However, their focus on individual utilities reflects a bygone threat era. The Department of Energy (DOE) *Cybersecurity Considerations* report[257] highlights a variety of ways in which adversaries could exploit DER common-mode failures and simultaneously disrupt distribution utilities across the United States. The lack

[254] NARUC, "Reliability."

[255] NRECA, *Facts and Figures*; and APPA, *Public Power.*

[256] This family of reliability metrics also includes equivalent frequency and duration assessments for distribution systems, versus customers (NARUC, "Reliability").

[257] DOE, *Cybersecurity Considerations*.

of interconnections between distribution systems (and their resulting immunity to cascading failure) offers no value against such widely shared threats.

Reliability stakeholders for distribution entities, including traditional utilities, aggregators, virtual power plants (VPPs), and their regulators, should supplement their existing reliability definitions and metrics with ones that account for the systemic threats to US power distribution, and they should apply those metrics to assess the prudence and costs avoided by investments to counter those threats. The same metrics will be useful for assessing initiatives to strengthen the resilience of power restoration capabilities, including via the deployment of grid-forming (GFM) inverters on batteries.

Building Nationwide Standards

The regulatory divide between the BPS and distribution systems is not the only impediment to developing and enforcing more consistent cybersecurity requirements across the electric system. At the distribution level, authority over utilities is splintered in terms of geography and by ownership model, with rural cooperatives, public power, and investor-owned utilities all overseen by different sets of authorities and regulators. Building consensus among these disparate entities to develop consistent mandatory DER standards (and enforcing those standards on aggregators and VPPs via interconnection agreements) will require new types of collaboration. Moreover, even for the BPS, additional measures are needed to establish nationwide standards—including for likely targets of People's Republic of China (PRC) cyberattacks.

Extending BPS Standards to High-Risk States and Territories

The unified but geographically constrained regulatory structure of the BPS is no accident. In response to the cascading failures and wide-area outages of the August 2003 blackout, Congress simplified that problem for the BPS. The Energy Policy Act of 2005 and section 215 of the Federal Power Act entrusted FERC with (i) approving and enforcing rules to ensure the reliability of the BPS; and (ii) certifying an electric reliability organization that would be charged with developing and enforcing mandatory reliability standards, subject to commission approval, and assessing reliability and adequacy of the BPS in North America. FERC certified NERC as the electric reliability organization in 2006, and they have collaborated on measures to strengthen reliability for BPS entities ever since.[258]

The geographic scope of NERC's responsibilities helps it address emerging cyber-related threats to reliability in a centralized, *almost* nationwide manner. Consistent with the Federal Power Act, NERC's jurisdiction excludes Hawaii, Alaska, and Guam.[259] Electric utilities in Hawaii will be in the bull's-eye of PRC efforts to disrupt the flow of forces in a Taiwan contingency. Alaska has infrastructure that is vital to national security as well. Nitin Natarajan, deputy director of the Cybersecurity and Infrastructure Security Agency (CISA), warns that Alaska faces intensifying cyber threats and that security initiatives in that state "have an impact on national homeland security and national defense."[260]

[258] FERC, "Reliability Explainer."

[259] FERC, "Reliability Explainer."

[260] Maxwell, "Threats Are Rising and Alaska Is Not Immune."

From a narrow structural perspective, excluding both states from NERC's operating reliability standards makes sense; neither has transmission systems that are interconnected with the three major US interconnections, so they cannot create cascading failures across the BPS. In terms of security, however, their exclusion advantages the PRC. Congress should amend the Federal Power Act to make Alaskan and Hawaiian high-voltage systems and associated control centers subject to NERC's critical infrastructure protection standards and should modify the act's definition of Defense Critical Electric Infrastructure to include those systems.[261]

Nevertheless, with Texas as a special case,[262] NERC's existing jurisdiction over the contiguous forty-eight states already enables it to provide consistent and continuously updated requirements for the entire BPS, including measures to deal with the reliability problems created by IBRs.[263] The regulatory environment is much more complex and challenging for efforts to secure DERs.

Distribution-Level Collaboration

NARUC emphasizes the value of having consistent (though voluntary) cybersecurity baselines across the United States. The association states that "a state-by-state approach to cybersecurity for the distribution grid" could "introduce inconsistencies and added complexity for owners and operators—many of whom manage distribution system assets in more than one state." Moreover, "a patchwork approach where states implement bespoke requirements would be more costly for owners and operators and their ratepayers."[264]

The need for a unified approach to DER security exists not only across multiple states and territories but also between different types of DER owners and operators. There is no single authority to establish and enforce standards for local distribution systems, rural cooperatives, and public power utilities. Public power utilities are entities of local or state governments and are typically regulated by elected or appointed boards, mayors, or city council members. Rural electric cooperatives are private, not-for-profit businesses. They are owned by their consumer members, who elect governing board members and are required to return any excess revenue to their members.[265] Investor-owned utilities (IOUs) are private, for-profit enterprises that are regulated at the distribution level by state PUCs. Some rural cooperatives and IOUs also operate high-voltage transmission systems and other BPS assets, making them subject to NERC reliability standards as well.

This diversity magnifies the problems created by the sheer numbers of distribution entities and the authorities who oversee them. All fifty states, the District of Columbia, and US territories have PUCs that

[261] EAC, *Strengthening the Resilience*.

[262] The Electric Reliability Council of Texas (ERCOT) is regulated by the Texas Public Utilities Commission, not FERC, because (per the commission) ERCOT's grid "is not connected to those of other states. Thus, power sales in ERCOT are not considered sales in interstate commerce and not subject to federal (FERC) oversight." However, all BPS entities in the ERCOT region are required to register with NERC and comply with NERC's mandatory reliability standards (FERC, *Introductory Guide*; and Texas RE, "Registration and Certification"). Some FERC commissioners suggest reassessing whether certain FERC regulations should apply to ERCOT given the growth of interstate transfers of power, especially to meet grid emergencies in Texas (see Morehouse, "Congress, Texas Should 'Rethink'").

[263] NERC, *Performance Assessment*, 15, 33–36.

[264] NARUC, *Scope And Prioritization of the Baselines*, 4.

[265] APPA, *Public Power*, 2; and NRECA, "What We Do."

independently rule on reliability and cybersecurity issues for sixty-four IOU holding companies, many operating distribution utility components in multiple states. Officials who oversee the reliability of over nine hundred rural electric cooperatives in forty-eight states have similar independence, including a significant number of small co-ops that serve important US military installations.[266] The same is true of officials responsible for approximately two thousand public power utilities that serve forty-nine states and the multiple US territories.[267] Among the latter is Guam—a focus of PRC Volt Typhoon grid compromise operations and likely a top priority for grid attacks in future Chinese conflicts with the United States.

It would be a nightmare for each of these thousands of entities to devise different reliability and security requirements for the solar systems, battery energy storage systems (BESS), and other products they purchase. Instead, to incentivize manufacturers of DERs to sell products that are secure by design (and also provide frequency support and other essential reliability services), the regulators and other officials responsible for overseeing distribution systems should mandate that only products that meet such standards be deployed on their systems. In turn, distribution systems could then require aggregators and VPPs to meet the same standards as a precondition to interconnect with them.

The quickest way to bridge the regulatory divisions between distribution entities would be for Congress to put all of them under the jurisdictions of FERC and NERC, which could modify emerging IBR mandates as needed for distribution systems and apply them nationwide to DERs. That option is a political nonstarter. Only a catastrophic event might drive legislators to abandon their long-standing support for state control of local distribution utilites. It is far better to avert such a catastrophe by developing new forms of security collaboration across the regulatory system we have today.

A more practical starting point would be to identify the NARUC cybersecurity baselines, National Institute of Standards and Technology (NIST) guidelines, Institute of Electrical and Electronics Engineers (IEEE) standards, and other voluntary measures that address the very most severe threats identified by DOE and the national laboratories. After transforming those voluntary guidelines into enforceable requirements, PUCs and their co-op and public power oversight counterparts could begin working further down the list of possible mandates on a risk-driven basis, with NERC's IBR standards providing an additional source of development options.

Three levels of coordination will be required to enable this conversion of voluntary to mandatory security requirements. First, to avoid the calamity of having fifty-four states and territories establish their DER standards, the systems' trade associations can seek agreement on potential standards from their respective members nationwide. Each of the three types of electric systems has its own "trade": the American Public Power Association (APPA), the National Rural Electric Cooperative Association (NRECA), and the Edison Electric Institute (EEI). NARUC also supports local distribution utilities on regulatory matters. All these organizations have deep expertise on the challenges facing their members and are best positioned to forge consensus between them on priorities for DER security requirements.

Second, to integrate the recommendations of the three trades, they should rely on the Electricity Subsector Coordinating Council (ESCC). The ESCC has never performed such a function in the past. However, in terms of official responsibilities and membership, it is uniquely suited to do so. The ESCC serves as the

[266] NRECA, *Electric Co-Op Facts and Figures*; and Cooperative.com, "Electric Co-Ops and the Military."

[267] APPA, "Our Members."

principal liaison between the federal government and the electric power industry on efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. A primary objective of the council is to "support collective efforts to strengthen the sector's security and resilience posture, as well as national security."[268]

ESCC's leadership structure is also ideal for building collaboration between the different types of distribution systems. Its executive committee includes chief executive officers (CEOs) from APPA, EEI, and NRECA. The ESCC has many other cybersecurity initiatives underway, including the growth of the Cyber Mutual Assistance (CMA) system.[269] Facilitating the development of industry recommendations on DER security mandates would be a logical extension of these efforts.

The third level of integration will be industry–government collaboration. While the ESCC serves as the industry's primary liaison with the federal government and coordinates with the Electricity Information Sharing and Analysis Center (E-ISAC), state and local leaders will also be crucial for shaping and enabling DER security mandates. The National Association of State Energy Officials (NASEO), the US Council of Governors, and other state and local leadership organizations should collaborate with regulators and industry trade associations to accelerate this progress, treating DER system reliability and cyber resilience issues with a priority that matches their importance to US national security.

Once in place, DER security mandates will overcome the temptation for distribution entities to buy products that are cheaper but more vulnerable than standards-compliant alternatives. But the increased costs of such security upgrades also create potential impediments to their deployment.

How Much, Who Pays, and for What?

Estimating the total costs of securing distribution systems against common-mode failures is difficult, especially if utilities, aggregators, and VPPs adopt the defense-in-depth strategies recommended by this study, which range from product gateways to secure DERMS. Each of these layers will entail their own costs. Moreover, a number of variables could drive those prices up or down. Tariffs or prohibition orders on high-risk Chinese products, including those proposed in the main report, could significantly increase costs. On the other hand, as voluntary guidelines (and, ideally, mandatory standards) expand the market for secure products, that increased purchase volume and predictability of demand is likely to drive down unit costs, further complicating assessments of systemic costs.

Despite these uncertainties, data points are emerging to assess the incremental costs of resilience upgrades. GFM inverters offer an especially useful example. Given the potential value of these advanced inverters to manage cyber-induced frequency and voltage disturbances, and—over the longer term—distribute and enhance the survivability of power restoration infrastructure and operations, BESS equipped with GFM capabilities are crucial for securing the decentralized grid.

The additional costs for these features (provided primarily by inverter software) are modest. Inverters designed for blackstart are only 2 to 5 percent more expensive than their grid-following (GFL) counterparts. The phasing of these software improvements will also affect incremental costs. From a system-wide

[268] CISA, *Electricity Sub-Sector Coordinating Council (ESCC) Charter*.

[269] ESCC, *Cyber Mutual Assistance Program*.

cost perspective, asset owners and operators can achieve significant savings by deploying GFM BESS as new projects go forward, versus retrofitting those capabilities later and incurring additional administrative, engineering, and system downtime costs. But some inverter experts anticipate that reprogramming GFM-equipped batteries would make them marginally more expensive by a few percent of the inverter's original cost.[270]

Assuming that the marginal costs for resilience and security upgrades are similarly modest for other DER systems (a big if), the question remains as to who should pay for these increased costs. DER project developers typically pay for the equipment and other expenses associated with their installations or are reimbursed by the military bases or other DER system hosts contracting for their services. But developers and DER advocates may seek to put utilities and their ratepayers on the hook for the costs of upgrading distribution infrastructure to accommodate those additional power flows. Such efforts are especially common if upgrades offer broader reliability improvements or if DER projects offer net benefits to ratepayers.[271]

Making ratepayers responsible for security upgrades will run into political and regulatory headwinds. NARUC, NRECA, and APPA and the authorities that oversee their member systems are committed to keeping power affordable. As one NARUC report frames the issue, "utility services are essential for health, safety, and the ability to fully participate in modern society. Affordability of energy bills is a priority consideration in decisions made by state public utility commissions and other decision-makers."[272]

Moreover, even modest incremental increases in ratepayer bills for DER security would pile on top of already rising electricity costs. The price US consumers pay for electricity is expected to rise in 2025 and likely beyond, driven by rising demand, transmission and distribution infrastructure investments, and an anticipated rise in the price of the natural gas that fuels much of US power generation. Based on US Energy Information Administration data, US electricity prices for all customer classes are expected to average 13.2 cents/kilowatt-hour in 2025, up from 12.68 cents/kilowatt-hour in 2023. Residential electricity prices across all regions will average 16.7 cents/kilowatt-hour in 2025, up from 15 cents/kilowatt-hour in 2022.[273]

These pressures on affordability make it imperative not only to require DER security investments on the highest-risk products but also to apply traditional regulatory assessment criteria for prudence to help winnow out gold plating and other unnecessary project costs. Some traditional criteria, including the need for projects to be "used and useful" in providing utility service to customers, are a poor fit to evaluate investments against future PRC attacks.[274] But NARUC and its partners have also developed energy resilience frameworks that are directly applicable to such assessments. These frameworks help regulators apply risk-based threat assessments and cost–benefit analysis to evaluate proposed investments, based in part on "costs avoided"—that is, the direct economic consequences of blackouts that would otherwise have occurred if a project did not go forward.[275] Such frameworks also enable the regulators to account for the

[270] Trabish, "Upgrading Inverters Is Urgent"; and Matevosyan, *Capturing the Reliability Benefits of Grid-Forming Batteries*.

[271] Kahrl et al., *Creating A National Initiative on DER Integration*.

[272] McCurry, *Customer Affordability and Arrearages*, 6.

[273] Walton, "Issues to Watch in 2025."

[274] Tietjen, "Tariff Development I," 4.

[275] McCurry and Nethercutt, "Developing a Shared Framework," 5–16.

indirect, societal costs (i.e., hospitals and fire and police stations without power) and the loss of service to "key military facilities"[276]—including those that PRC leaders will seek to disrupt by attacking the grid.

From an equity perspective, however, it might be better to adopt an additional rule of thumb: if projects directly (and primarily) protect the flow of power to specific defense installations or other facilities critical for national security, the federal government should fund those investments. If projects improve the reliability of service to all utility ratepayers in a given service area, the costs of those investments should be borne more broadly via tariffs, rate cases, and other established means of cost recovery. The latter approach to funding will be especially appropriate for investments that improve resilience against multiple hazards. We now have a historic opportunity to shape the grid's evolution, by employing DERs and IBRs that are both reliable and secure, to achieve such broader benefits.

[276] McCurry and Nethercutt, "Developing a Shared Framework," 12.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY