Weathering the Storm

STRATEGIC POWER ISLANDING AGAINST CASCADING BLACKOUTS

National Security Perspective

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

WEATHERING THE STORM

Strategic Power Islanding Against Cascading Blackouts

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

COMM-25-01394

Contents

Figures

Figure credits:

Figure 1: Figure adapted from "US Electric System Is Made Up of Interconnections and Balancing Authorities," EIA (US Energy Information Administration), July 20, 2016, https://www.eia.gov/todayinenergy/detail.php?id=27152; and Connor Waldoch, "SPP Expansion Provides a Blueprint for the Future of the Grid," Grid Status Exports blog, September 26, 2023, https://blog.gridstatus.io/spp-expansion-west/.

Figure 3: Information from EIA, https://www.eia.gov/electricity/state/; figure reproduced from EIA, "California Was the Largest Net Electricity Importer of Any State in 2019," December 7, 2020, https://www.eia.gov/todayinenergy/detail.php?id=46156.

Figure 4: "Interstate Natural Gas Supply Dependency, 2007," EIA, https://www.eia.gov/naturalgas/archive/analysis_publications/ngpipeline/dependstates_map.html.

Summary

The US power grid is superbly structured for peacetime but has a potentially catastrophic vulnerability in war. The grid is divided into three large electric transmission networks: the Eastern, Western, and Texas interconnections.[1] These interconnections tie together so many generators, transmission lines, and other assets that when natural hazards create blackouts, utilities can almost always keep them brief and limit their spread.

The exceptions, however, illuminate a danger for adversaries to exploit. As seen in the United States in 2003 and the Iberian Peninsula in 2025, uncontrolled blackouts can cascade across interconnected electric systems in seconds. When such cascades occur, interconnections shift from being a bulwark of resilience to a threat vector, jeopardizing the flow of power to military bases, water systems, and other critical loads.

The United States should prepare for that tipping point. Grid operators are ready to take emergency actions to prevent cascading outages and help interconnections survive if cyber and kinetic attacks create severe electric system disturbances. But if their actions prove inadequate and cascades are imminent or underway, the United States should be ready to separate the interconnections into multistate, preplanned power islands that are impervious to the spreading outages. This study proposes how to design and operate such islands and recommends criteria for deciding whether and when to separate them from surrounding electric systems.

Islanding cannot prevent the lateral movement of malware between utilities. That goal is best accomplished by grid-wide cybersecurity measures. Rather, by electrically separating islands from surrounding transmission and distribution infrastructure, those islands would become invulnerable to power swings, extreme voltage, and frequency disturbances, as well as other grid instabilities propagated by neighboring systems.

Microgrids offer a widespread but deficient islanding strategy. In emergencies, microgrids can separate from the grid and use their own generators and distribution systems to serve critical loads within their perimeters. However, they are usually too small to encompass the water utilities and other electricity-dependent infrastructure on which their critical facilities rely. In addition, given the cost of deploying new generators and other equipment that microgrids require, the United States will never be able to afford enough of them nationwide for defense against cascading failures.

This study recommends an alternative: configure islands around the existing service territories of multistate balancing authorities, which already have key authorities and capabilities to protect grid reliability. These "microgrids on steroids" would rely on existing generators and other infrastructure within their boundaries rather than require new construction and would encompass all of the interdependent infrastructure relied on by hospitals, seaports, and other vital defense and civilian facilities. These islands would

[1] The North American Electric Reliability Corporation (NERC) defines an interconnection as "a geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control." In turn, the bulk power system is defined as "(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 of Terms*, 24, 10.

also be strategically designed to counter the specific goals that the People's Republic of China (PRC) would seek to achieve by attacking the US grid.

Even the largest islands would have drawbacks compared with interconnections. Interconnected utilities can import and export power to each other to help manage disturbances and fill gaps in local power supplies. Utilities separated from the grid will be unable to do so. Indeed, in California and a few other regions, islands will never have sufficient generation to serve all the loads within them. Managers of those islands will need to prioritize service to critical facilities and leave many other customers in the dark, disrupting the economy and putting lives at risk.

Yet, the consequences of interconnection-wide outages could be worse, especially if (as examined in this report) adversaries sustain their attacks to disrupt and delay power restoration for weeks. The question is: under what circumstances is islanding the least bad option? Separation would make sense if, in the face of mounting instabilities and escalating sensor and equipment failures, grid managers determine that emergency actions can no longer prevent cascading blackouts. But given the astonishing speed with which cascades can spread, and the danger that adversaries will disrupt grid sensors and telemetry, relying on conditions-based criteria would be risky.

Instead, the president could order separation after determining that a potentially catastrophic attack is imminent or underway. Relying on intelligence and warning carries two risks: being caught by surprise or being spoofed into islanding when an adversary does not intend to attack. The United States can mitigate these dangers by issuing phased orders that (based on threat indicators) move from initial preparation for islanding to separation, equivalent to the Department of War (DOW) Force Protection Condition system that sequences threat response actions by installation commanders and other DOW personnel.[2]

Islanding offers potential benefits for deterrence as well. The US intelligence community has identified the goals that Chinese leaders will seek by attacking the US grid and other infrastructure, including inciting societal panic and interfering with the deployment of US forces.[3] If islanding can prevent cascading failures from disrupting service to key societal and military loads, we may be able to reduce Xi Jinping's confidence that he can achieve his objectives. The prerequisite: configuring strategic power islands to defend the American people and support national defense and convincing Xi and other potential attackers that we can operate islands under fire.

2 Pitts, "Force Protection Conditions."

3 ODNI, *Annual Threat Assessment*, 12.

People's Republic of China–Induced Cascading Failures

Transmission system operators (TOPs) and other components of the bulk power system (BPS) are laser focused on maintaining the reliable operation of the electric grid and preventing cascading failures—that is, "the uncontrolled successive loss of system elements" that results in widespread blackouts which "cannot be restrained" from spreading.[1]

Grid operators have extensive plans and capabilities to prevent disruptive events from sparking cascades. And when cascades nevertheless occur, as in the US Southwest in 2011 and the Iberian Peninsula in 2025, operators closely study those failures to bolster their prevention measures. But all of these past events have occurred without enemy "help." The People's Republic of China (PRC) is rapidly improving its cyber and kinetic attack capabilities, with unmanned aerial systems (UASs) facing near-zero grid defenses. Moreover, Chinese researchers are studying how to target these attacks to create cascading outages, especially in the Western Interconnection, which powers seaports and other infrastructure crucial for deploying US forces to East Asian conflicts.

Attackers can also exploit dangers to the grid of our own making. The North American Electric Reliability Corporation (NERC) is responsible for assuring the effective and efficient reduction of risks to the reliability and security of the North American BPS.[2] NERC's president, Jim Robb, notes that an "escalating toxic soup" of physical and cybersecurity risks constitutes only part of the challenge of securing the grid. Other factors are also contributing to "a five-alarm fire when it comes to reliability," including dwindling resource adequacy, weakening reliability services, the growing complexity of the grid's architecture, and the rise of new (and poorly secured) attack surfaces.[3] This combination of rising threats and expanding vulnerabilities is creating new opportunities for the PRC to inflict cascading blackouts across our interconnections.

Russia, North Korea, Iran, and other potential adversaries could seek to create cascading failures as well. This study focuses on China as "the most persistent cyber threat to U.S. government, military, and civilian networks."[4] However, many of the study recommendations will be useful against other adversaries as well, particularly as artificial intelligence (AI) helps enable such attackers to create and propagate grid disruptions.[5]

Cascades Past and Future

NERC and the Federal Energy Regulatory Commission (FERC) establish mandatory, enforceable grid reliability standards for BPS entities, including many standards that are specifically designed to prevent disturbances from spreading.[6] *Standard TOP-001-6—Transmission Operations*, for example, is intended to "prevent instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Interconnection by

[1] NERC's full definition of cascading is "the uncontrolled successive loss of System Elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies." See NERC, *Glossary of Terms*, 24, 10.

[2] NERC, "Who We Are."

[3] Howland, "NERC President Warns of 'Five-Alarm Fire.' "

[4] DOW, *2025 Annual Report*, 17.

[5] This study follows the definition of AI provided in 15 U.S.C. § 9401: "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- (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."

[6] See, for example, *PRC-027-1*, which is designed to "maintain the coordination of Protection Systems installed to detect and isolate Faults on Bulk Electric System (BES) Elements, such that those Protection Systems operate in the intended sequence during Faults." NERC, *PRC-027-1*.

ensuring prompt action to prevent or mitigate such occurrences."[7] To limit the spread and severity of instabilities that occur, TOPs and other grid operators must implement an array of additional emergency operations (EOP) standards, which are designed to help the BPS "withstand disturbances in anticipation of potential events, manage the system after an event, and/or prepare to restore or rebound after an event."[8] NERC and FERC also issue and regularly update critical infrastructure protection (CIP) standards, which require specific measures to defend the grid against physical and cyber threats.

These measures reduce but cannot eliminate the risks posed by cascading failures. The ways that cascades have occurred in the past help illuminate how sophisticated adversaries can seek to create them today and why the United States needs new fallback defenses that can mitigate the effects of such blackouts.

Conservative Operations and Emergency Actions

Grid operators have increasingly sophisticated grid sensors, including phasor measurement units (PMUs), to help them detect, assess, and respond to grid emergency conditions. AI-enabled modeling and simulation (M&S) tools, digital twins of electric systems, and other decision-support systems can help grid personnel assess incidents and optimize responses to them.[9] Together with advances in energy management systems (EMS), supervisory control and data acquisition (SCADA) systems, and other situational awareness and control tools, grid operators are better equipped than ever before to manage dangerous grid conditions and prevent cascading failures.

These mitigation measures will offer a key line of defense against PRC-induced instabilities. In an intensifying US–China crisis, just as with an approaching hurricane, grid managers can prepare for possible system disruptions by transitioning their systems to conservative operations, staffing up their emergency operations centers, and taking other measures.[10] Once events are underway, operators can employ an extensive array of emergency actions to limit disruptive effects. NERC standards specify the measures that grid operators will take. Standard *EOP-002-3.1—Capacity and Energy Emergencies* states that "each Balancing Authority and Reliability Coordinator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its respective area and shall exercise specific authority to alleviate capacity and energy emergencies."[11] These actions include but are not limited to:

- Loading all available generating capacity
- Deploying all available operating reserve
- Interrupting interruptible load and exports
- Requesting emergency assistance from other balancing authorities (BAs)
- Conducting underfrequency load shedding so that a BA and transmission operator operating with insufficient generation or transmission capacity can (and indeed, must) conduct load shedding rather than risk cascading failures.[12]

[7] NERC, *TOP-001-6*, 1.

[8] NERC, *Reliability Issues Steering Committee*, 8. These NERC standards include *BAL-003-2*, *PRC-006-2*, and many other standards for emergency planning and operations.

[9] Biswas et al., *Big Data Analysis*, 8–12; Hayat et al., "Expert and Intelligent Systems"; and e-Magic, "Silent Power Crisis."

[10] Many reliability coordinators and BAs offer definitions of conservative operations similar to that provided by SERC Reliability Corporation: "This mode of preparation or operation of a power system for an expected, impending, or occurring event or power system condition is designed to lessen risks and reduce impact to the reliability of the power system due to the event or power system condition." SERC, *Guideline: Conservative Operations*, 4.

[11] NERC, *EOP-002-3.1*, 4.

[12] Manual load shedding provides grid operators with a less draconian—and more selective—option for addressing generation–load imbalances. Manual load shedding is dis-

Large-scale load shedding can cause massive economic losses and threaten public safety. Nevertheless, if such extraordinary measures can stave off cascading outages, their benefits will outweigh their costs. The 2021 Texas outage exemplifies those benefits. In that winter storm event, draconian load shedding staved off a potential cascading blackout across the entire Electric Reliability Council of Texas (ERCOT) service area that could have lasted for weeks or more before power was fully restored.[13] These same actions will prove useful against cyber-induced instabilities, especially when paired with defensive measures against such attacks.[14]

The ways that cascades have occurred in the past help illuminate how sophisticated adversaries can seek to create them today.

Conservative operations are not guaranteed to stave off cascading failures. In the final report on the Iberian Peninsula blackout, regional regulators, power companies, and technical experts found that emergency load shedding and other "system defence plans in Spain and Portugal were automatically triggered by the drop in frequency in the final stages leading up to the blackout. They were unable to prevent the system's collapse, despite the fact that their activation proceeded as designed."[15] NERC, FERC, and BPS entities are continuously drawing lessons learned from such failures and are strengthening grid defenses accordingly. After every cascading outage since the massive 2003 blackout, which spurred Congress to authorize FERC and NERC to mandate and enforce reliability standards, these regulators have analyzed the causes of cascades and (with input from power companies) developed initiatives to prevent them in the future.[16]

The Next Cascade

A notable feature of all of these blackouts: none of them stemmed from cyber or physical attacks. Cascading outages have rippled across the US interconnections because of failures to maintain sufficient reactive power support, warning system malfunctions, failures to operate the grid within secure limits, inadequate regional situational awareness by grid managers, and other causes, all of which have contributed to massive blackouts without enemy actions to spark or exacerbate their spread.[17]

Adversaries seeking to create and widen the scope of such blackouts could seek to exploit all of these failure modes. In addition, they could target protection systems to further trigger and expand cascading outages. Protection systems are vital for grid resilience. Extreme frequency and voltage disturbances can damage transformers, transmission lines, generators, and other grid equipment—for example, frequency excursions can break generator blades. Protection systems prevent such damage. When unstable power swings occur, protective relays, circuit breakers, and other protection systems disconnect (or "trip off") equipment from the grid.[18] These protective measures are crucial to limiting the impact of cascading failures. As long

cussed in the section on strategic power islanding. NERC, *EOP-011-4*; and NERC, *PRC-006-NPCC-2*.

[13] FERC, *February 2021 Cold Weather Outages*, 4, 127, 152–155. On the multiple weeks required for blackstart power restoration and the potential economic consequences of an ERCOT-wide blackout, see *Power Struggle*, 2.

[14] NERC, *CIP-008-7*.

[15] ICS Investigation Expert Panel, *Final Report*, 21–22. Additional analysis of the blackout causes and recommendations for improvements against cascading failures can be found on pp. 451–461.

[16] For a prime example of such analysis, see FERC and NERC, *Arizona-Southern California Outages*.

[17] The US–Canada report on the August 14, 2003, blackout details all of these causal factors, many of which have played significant roles in subsequent blackouts. US-Canada Power System Outage Task Force, *Final Report*, 18–19, 139.

[18] NERC, *Glossary of Terms*, 32.

as protection systems enable generators and other equipment to survive such events without damage, those assets can help restore service when a blackout is over and thereby limit the consequences of an outage.[19]

However, the benefits of protection systems have a flip side in cascading events. These systems can trigger additional failures and greatly increase the scale of blackouts. The US–Canada report on the 2003 blackout summarizes this process. The process begins with an initial disturbance of grid equipment such as when, in 2003, transmission lines touched overgrown trees and tripped off.[20] The next phases unfold as follows:

> Power swings and voltage fluctuations caused by these initial events can cause other lines to detect high currents and low voltages that appear to be faults, even if faults do not actually exist on those other lines. Generators are tripped off during a cascade to protect them from severe power and voltage swings. Protective relay systems work well to protect lines and generators from damage and to isolate them from the system under normal and abnormal system conditions. But when power system operating and design criteria are violated because several outages occur simultaneously, commonly used protective relays that measure low voltage and high current cannot distinguish between the currents and voltages seen in a system cascade from those caused by a fault. This leads to more and more lines and generators being tripped, widening the blackout area.[21]

Cascading blackouts offer the PRC a uniquely efficient way to achieve its goals in future conflicts.

Relay tripping intended to protect equipment helped spread outages across the Iberian Peninsula in 2025. The Final Report on the causes of that outage, written by regional regulators, power companies, and technical experts, found that "the blackout occurred after an uncontrolled, rapid rise in system voltage and loss of voltage control on a day with multiple concurrent phenomena, accelerated by rapid generation output reductions and disconnections, leading to voltage instability and cascading generation disconnections in Spain."[22] NERC's assessment of the event reached similar conclusions, including the role played by the failure of hydropower and other conventional generators to absorb excessive reactive power as they were supposed to do. However, Mark Lauby, NERC's senior vice president and chief engineer, stresses the importance of an additional factor: as disturbances spread, high voltages caused generators to trip protectively and shut down, putting more stress on the network and pushing systems toward automatic shutdown levels. "It's kind of a death trap at that point," Lauby added.[23]

[19] US-Canada Power System Outage Task Force, *Final Report*, 91.

[20] Two significant events preceded the transmission line event and made it more difficult to manage: inaccurate input data rendered the independent system operator's state estimator (a system monitoring tool) ineffective, and the alarm and logging system in the area TOP's control room failed and was not restored until after the blackout. Subsequent portions of this section discuss the significance of both events as potential attack vectors. US-Canada Power System Outage Task Force, *Final Report*, 45.

[21] US-Canada Power System Outage Task Force, *Final Report*, 73–74.

[22] ICS Investigation Expert Panel, *Final Report*, 6. Additional analysis of the blackout causes and recommendations for improvements against cascading failures can be found on pp. 451–461.

[23] Behr, "Spain's Big Blackout." For additional details on the role of inadequate voltage controls and shortfalls in reactive power margins, which "could have prevented system collapse," see ICS Investigation Expert Panel, *Final Report*, 22.

Again, enemy attacks played no role in exacerbating this process or (as occurred in the Southwest US blackout of September 2011) in establishing faulty relay settings that triggered unnecessary interruptions.[24] But adversaries can develop tools that leverage the peacetime causes of cascading outages, and—with the help of AI—conduct precisely targeted cyber and kinetic attacks to create and lengthen the duration of interconnection-wide blackouts.

Intensifying Threats and Expanding Attack Surfaces

In the past decade, dozens of Chinese researchers have published academic studies on how cascading failures propagate through the US grid and how to optimize cyberattacks to create such outages and magnify their geographic scope.[25] Some of these reports frame their analyses as "red team" efforts to support defensive measures. US electric industry personnel conduct equivalent defensive work on a sustained basis. However, by conducting simulations to identify the most efficient attack vectors to trigger large-scale blackouts, the analysis produced by some of these Chinese researchers could have offensive applications as well. Among the notable examples:

- A 2022 study emphasizes the value of identifying "the key substations or destructive nodes to destroy the power grid" and offers methodologies for conducting that analysis. The study then applies those methodologies to "node data from Western United States power grid" to identify destructive nodes and evaluate how disrupting them would impact the grid.[26]
- A 2011 report investigates "the performance of the power grid of the western United States subject to three intentional attacks" and assesses the effectiveness of those attack vectors in creating cascading failures.[27]
- A 2020 publication applies modeling techniques to cascading failures in the US grid and proposes how use of the model can "significantly improve the destructiveness of complex networks against cascade failure."[28]

Other Chinese studies identify additional attack vectors for creating wide-area blackouts. A 2025 analysis by a US threat intelligence company found that from 2010 to the present, PRC-based organizations published over 2,700 reports examining US grid vulnerabilities and ways to exploit them.[29]

The PRC may structure attacks early in a confrontation to create small-scale disruptions rather than cascading failures (though due to complex grid dynamics, even constrained strikes could produce outages greater than China intends). DOW states that China's People's Liberation Army has considered the possibility of conducting limited "demonstration" cyberattacks against a small set of targets to create "clear awing effects" on the United States.[30] And if PRC leaders wanted to disrupt a larger number of assets to increase those awing effects, AI could help them plan and execute individualized attacks at scale instead of indiscriminate, interconnection-wide outages.

Nevertheless, cascading blackouts offer the PRC a uniquely efficient way to achieve its goals in future

[24] FERC and NERC, *Arizona-Southern California Outages*, 101. In the November 1965 Northeast blackout, low settings on Zone 2 relays on lines leaving an Ontario hydro plant helped initiate the event. Federal Power Commission, *Northeast Power Failu*re, 6–8.

[25] Erika Langerová, a cybersecurity researcher at the Czech Technical University, has published a valuable compendium of Chinese-authored studies on cascading failures. See Langerová, "China Is Studying.".

[26] Yu et al., "Selection of the Disruptive Nodes."

[27] Wang and Rong, "Robustness of the Western United States Power Grid."

[28] Chen et al., "Nonlinear Model of Cascade Failure."

[29] Striderintel.com, *In Broad Daylight*, 7.

[30] DOD, *Military and Security Developments*, 95.

conflicts. The Office of the Director of National Intelligence (ODNI) offers the following assessment of those objectives:

> If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.[31]

The ability to create cascading failures would obviate the need to tailor and coordinate attacks against a large number of individual grid assets. In one fell swoop, ports, rail infrastructure, and other facilities and functions essential for deploying forces to the Taiwan Strait or other conflict zones would lose the power on which they depend. Thousands of water utilities and other systems essential for public health and safety would lose service as well, heightening US decision-makers' perceived costs of defending American allies against China.

PRC Cyberattack Capabilities

China has also been strengthening its capabilities to conduct such attacks. DOW notes that China has "burrowed" compromise into US infrastructure via the Volt Typhoon campaign and continues "building cyber capabilities for future use in crisis or conflict, including for disrupting the U.S. military's ability to mobilize in conflict."[32] US electric systems are also riddled with Chinese-produced batteries, power inverters, transformers, and other equipment that pose potential attack opportunities nationwide. *Surfing the Wave: Resilience Strategies for the Decentralizing Grid* examines how the PRC could use these threat vectors (as well as load-manipulation attacks) to create severe, interconnection-wide frequency and voltage disturbances.[33]

Since the publication of that report, additional data have emerged on the risks posed by supply chain compromises. More than 85% of the utilities surveyed for a recent industry report rely on inverters made by companies with ties to the PRC government and military, all of which can be accessed remotely.[34] Other Chinese-produced grid components could enable multiregion attacks as well. The US-China Economic and Security Review Commission found in November 2025 that "over 90 percent of all power electronics, battery technology, control components, and electronic sensors contain at least one critical component sourced from China, and at least 70 percent are fully made in China."[35]

AI will also enable China to more precisely map the grid's critical nodes and choreograph attacks to maximize the effects of disrupting those assets.[36] Advances in such reconnaissance and in AI-enabled M&S of the US electric system can help the PRC pinpoint bottlenecks in transmission systems, exploitable infrastructure configurations, and other factors to help design attacks tailored for cascading effects.[37]

31 ODNI, *Annual Threat Assessment*, 12. ODNI's *2026 Annual Threat Assessment* offers less-specific descriptions of PRC attack objectives.

32 DOW, *2025 Annual Report*, 18.

33 Stockton, *Surfing the Wave.*

34 Striderintel.com, *In Broad Daylight*. For the exploitable features of inverters produced by specific Chinese companies, see Dashevskyi, La Spina, and dos Santos, *SUN:DOWN*. On the risks that China will exploit inverters to create cascading failures, see Halper and Nakashima, "This One Gadget."

35 USCC, *2025 Report to Congress*, 562.

36 On the value of AI for reconnaissance as well as other components of the cyber kill chain, see Danzig, *Artificial Intelligence*, 14–25.

37 On congestion and the increasing number and severity of US transmission system bottlenecks, see Fuzaylov, "Why Transmission Congestion Matters." On the role bottlenecks can play in cascading outages, see Anvari and Vogt, "Identifying the Power-Grid Bottlenecks, 516–517.

AI will also help adversaries design and conduct cyberattacks to exploit all of the failure modes that helped create and widen the geographic scope of previous cascading blackouts, as well as new attack vectors. The National Security Commission on Artificial Intelligence found that AI 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."[38] AI will help the PRC employ many of the failure modes that contributed to previous cascading failures—denial or corruption of situational awareness, loss of reactive power, malfunctioning of alarm systems, misoperation of protection systems, etc.—with greater effectiveness, simultaneously, and across massive numbers of digital grid systems.

A July 2025 study by Richard Danzig, former secretary of the Navy, examines additional ways in which advances in large language models (LLMs) and other AI tools will strengthen the design and execution of cyberattacks. LLMs, for example, "are likely to amplify operationally useful intelligence by more than seven or eight orders of magnitude."[39] Subsequent reports determined that a Chinese state–sponsored organization is already applying such advances across the attack life cycle, using code from Claude (an LLM) to penetrate government agencies and major technology corporations.[40] Especially concerning: as tools like Anthropic's Mythos AI tool demonstrate, we must assume that the PRC will gain unprecedented capabilities to discover zero-day exploits on US grid control software and employ that knowledge to develop new plans to trigger and sustain cascading failures.[41]

US power companies should respond to these developments by accelerating the adoption of AI tools to bolster their defenses and secure those tools from adversary manipulation and corruption.[42] In the meantime, AI will continue to help the PRC precisely map ways to create cascading failures across the three interconnections and exploit the attack opportunities enabled by compromised PRC equipment, Living off the Land (LotL) techniques, and large-scale load manipulation.

Kinetic Threats

Although staying ahead of intensifying PRC cyber threats poses a difficult challenge, the gap between adversary capabilities and US preparedness is far wider with respect to physical attacks. NERC standard *CIP-014-3—Physical Security* required transmission system owners and operators to "identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection."[43] So far, so good.

The problem lies in how NERC and its industry partners are implementing this requirement. NERC's *Draft Security Guideline* (September 2025) describes the defensive measures that transmission system owners and operators typically adopt to comply with CIP-014-3 and related physical security mandates. These defenses include chain-link fences, palisades made of vertically placed stakes,

[38] NSCAI, *Final Report*, 50–51.

[39] Danzig, *Artificial Intelligence*, 9.

[40] Anthropic, *Disrupting*. For an assessment of the validity of Anthropic's findings, which have not yet been confirmed by US government agencies, see Brumfield, "Ignoring AI."

[41] On Mythos and its implications for developing zero-day attacks, and on Project Glasswing, which seeks to strengthen defenses against such attacks, see Roose, "Anthropic Claims Its New A.I. Model"; Anthropic, *Project Glasswing*; and Evron, Mogull, and Lee, "'AI Vulnerability Storm.'"

[42] DOE, *Potential Benefits and Risks of Artificial Intelligence*; and Stockton, *Surfing the Wave*, Appendix B.

[43] NERC, *CIP-014-3*.

bollards and other vehicle barriers, and LED area lighting that "improves perceived and actual security."[44]

All of these measures strengthen the security of critical substations and other assets against high-powered rifles and other familiar threats. They are totally useless, however, against UASs (a.k.a. drones) that will fly over fences to destroy substation transformers and other costly, difficult-to-replace equipment. The Cybersecurity and Infrastructure Security Agency (CISA) warns that Chinese-manufactured UASs deployed across the United States pose a significant risk to critical infrastructure and US national security.[45]

These risks are growing. In January 2026, DOW warned that "the operational landscape has fundamentally and irrevocably changed. The proliferation of inexpensive, capable, and weaponizable unmanned aerial systems (UAS) by both peer competitors and non-state actors presents a direct and growing threat" to US military bases.[46] The severity of that threat was highlighted in March 2026 when multiple waves of UASs overflew Barksdale Air Force Base in Louisiana, which houses long-range B-52 bombers and plays a critical role in command and control of the Air Force nuclear defense capabilities.[47]

The same dangers confront the electricity substations and other infrastructure serving Barksdale and other vital military and civilian facilities. UAS capabilities to operate autonomously as part of coordinated swarms against multiple targets will magnify these risks and increase the difficulty of countering drone attacks.[48] And thanks to Ukraine's Operation Spider's Web, we now have a real-world example of how covertly deployed UASs can conduct such coordinated strikes across many thousands of square miles.[49]

NERC's *Draft Security Guideline* report notes that a "racially motivated violent extremist" was arrested in November 2024 for attempting to attack a Nashville-area substation with an explosives-laden drone and that "evolving drone technology makes it easier for drones to carry and deliver more sophisticated payloads."[50] PRC attacks employing such payloads, conducted at scale against substations selected to create cascading failures, pose immensely greater dangers. Yet, NERC's ongoing *Draft Security Guideline* initiative to update physical standards does not propose requirements to counter UASs.[51] The standards revision process should fill these gaps as quickly as possible. Until then, BPS standards will continue to shoot behind (or rather, under) the target.

The greatest danger posed by UAS threats lies in the extended duration of the outages they could create.

Congress has created a more immediate opportunity to defend electric infrastructure from drone attacks. The Safer Skies Act, which became law in December 2025, greatly expands the authority of local, state, and federal law enforcement agencies to help protect critical grid assets in ways that go beyond drone detection and tracking. After State, Local, Tribal, and Territorial (SLTT) law enforcement agency personnel complete the training specified by the act, they can take such actions that are "necessary to mitigate a credible threat

44 NERC, *Draft Security Guideline.*

45 CISA, *Release Cybersecurity Guidance.*

46 DOW, "JIATF-401 Announces Updated Guidance."

47 Margolin and Katersky, "'Multiple Waves' of Unauthorized Drones."

48 On these technical advances and the resulting problems for defense against UASs, see Cox, "Many US Bases Still Lack Sufficient Tech."

49 Collett-White, Dutta, and Zafra, "How Ukraine Pulled Off an Audacious Attack."

50 NERC, *Draft Security Guideline*, 28. See also DOJ, "Man Pleads Guilty."

51 NERC, *Project 2023-06 CIP-014.*

that an unmanned aircraft system or unmanned aircraft poses to the safety or security of people, facilities, and assets, a venue or set of venues used for large-scale public gatherings or events, *critical infrastructure*, or correctional facilities" (emphasis added).[52]

As long as critical substations and control centers remain defenseless against UAS attacks, the electric industry and its government partners should strengthen US capabilities to stanch the spread of kinetic-induced instabilities.

Electric utilities already have strong collaborative relationships with SLTT law enforcement agencies, including for assistance against high-powered rifle attacks and other traditional kinetic threats. Utilities should build on those foundations, and on Safer Skies implementation measures to protect US World Cup venues in 2026, to coordinate with law enforcement partners for grid defense.[53]

However, given the competing demands for law enforcement support, defending even a limited number of substations around the clock would be difficult for all but the largest agencies. Moreover, Safer Skies authorizes only countermeasures that exploit the dependence of UASs on radio frequency communications. Following the lead of Ukraine and Russia, the PRC is likely to move toward increasingly autonomous, AI-enabled drones that do not need sustained communications to strike their grid targets. Countering such advanced UASs will be vastly more difficult, and will likely require the adoption of DOW-equivalent lasers or other shoot-down capabilities that would take years for law informant agencies (much less utilities) to effectively deploy.

Another defensive option is to choke off US customers' access to potentially exploitable drones manufactured by DJI and other Chinese companies. On December 22, 2025, the US Federal Communications Commission prohibited drones and drone components produced by China's DJI and other specified foreign companies from "being imported for use or sale in the U.S."[54] That is a much-needed step. But hundreds of thousands of Chinese-produced UASs are still flying across the United States and "benefiting" from repeated firmware updates and sustained communications links back to China.[55] Moreover, given the risk that adversaries will smuggle increasingly sophisticated drones and/or their components into the United States and (as exemplified in Russia's war against Ukraine) improvements in the autonomous operation of UASs across vast distances, threats of kinetic attacks against US grid infrastructure will continue to intensify.[56]

The PRC's ability to create cascading failures via UAS attacks benefits from an additional factor: near-perfect knowledge of critical grid nodes. US grid infrastructure includes over 55,000 electricity substations and 642,000 miles of high-voltage lines. Conducting simultaneous attacks against all of these assets would present a formidable challenge, even with the help of AI and massive drone fleets.[57] But such nationwide strikes are not necessary to create cascading outages.

In many US regions, relatively small numbers of electricity substations and transmission lines are vital for importing power to meet demand, maintaining reliable service, or (via the distribution systems they feed) serving military and civilian loads

52 National Defense Authorization Act for Fiscal Year 2026, § 8601.

53 For an example of such World Cup defenses, see Chapman, "LAPD Secures $9.8 Million DHS Grant."

54 FCC, "FACT SHEET."

55 Singh, "DJI Pushes Massive Firmware Update."

56 Chivers, "In Ukraine."

57 DOE, "Achieving American Leadership."

that China will seek to disrupt. Massive amounts of publicly available data help the PRC map these assets.[58] Chinese reconnaissance satellites, thefts of protected utility data, and surveillance by PRC-produced UASs can provide additional information, with AI helping determine which targets to prioritize for attack in order to initiate and expand cascading outages.

Yet, in terms of attack consequences, the greatest danger posed by UAS threats lies in the extended duration of the outages they could create. Utilities and their government partners have built sophisticated capabilities to hunt for and remediate malware on cyber-enabled infrastructure and—ideally—will be able to rapidly restore the functionality of those systems if blackouts occur.

The physical destruction of large power transformers (LPTs) and other critical grid equipment presents a different challenge. The Department of Energy (DOE) notes that LPTs "are expensive, difficult to transport, and typically custom-made with procurement lead times of one year or longer."[59] The Spare Transformer Equipment Program and other initiatives provide mechanisms for participating entities to share assets in the event existing equipment is deliberately destroyed.[60] In addition, the Transformer Transportation Working Group provides guidance on how to obtain support from government and private-sector transportation partners during incidents that require the emergency movement of LPTs, including via the specialized railcars that transport these multiton assets. However, if a UAS attack destroys large numbers of LPTs and disrupts the flow of power on which transportation systems depend, it could take many weeks or even months to get critical substations back up and running.

[58] See, for example, Deming, "Grids and Generators."

[59] DOE, "Addressing Security and Reliability Concerns."

[60] EEI, *Spare Equipment;* and EEI, *EEI Emergency Response.*

The severity of the UAS threat makes it imperative to devise solutions to these problems. The electric industry should consider borrowing from the innovative resilience measures being employed by Ukraine and the Baltic states against UAS and missile attacks, including the dispersal of assets to complicate enemy targeting and accelerate power restoration.[61] Utilities should also explore how to leverage Department of Homeland Security counter-UAS (C-UAS) programs and technologies that DOW is developing to protect military bases at home and abroad.[62] FERC and NERC will also need to enable utilities to recover the costs of deploying counter-drone defenses.

In the meantime, as long as critical substations and control centers remain defenseless against UAS attacks, the electric industry and its government partners should strengthen US capabilities to stanch the spread of kinetic-induced instabilities—including the measures examined in the sections on current fallback defense and strategic power islanding in this study.

New Vulnerabilities for PRC Exploitation

FERC defines the reliable operation of the grid as "operating the elements of the bulk-power 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."[63] NERC's assessment that we face a five-alarm fire when it comes to reliability reflects that new

[61] Sytas and Strzelecki, "On NATO's Eastern Flank." For a summary of Ukraine's measures to strengthen grid resilience against UAS attacks, including by decentralizing and dispersing generation resources, see Stockton, *Surfing the Wave*, 20–21.

[62] DHS, *Counter-Unmanned Aerial Systems*; Pomerleau, "DOD Creating Joint Interagency"; and DOD, "FACT SHEET."

[63] FERC, *Reliability Primer*, 39. This definition is derived from the one established by Congress in the Federal Power Act. See 16 U.S.C. § 824o–1.

grid vulnerabilities have emerged for adversaries to exploit.

BPS entities and government partners are striving to mitigate these risks. One indicator of progress is industry's ability to anticipate and protect against the failure modes that contributed to the 2025 Iberian Peninsula blackout. A key feature of the US grid's transformation lies in the deployment of tens of millions of solar-generation resources and other inverter-based resources (IBRs). When the initial disturbance in the Iberian blackout occurred, IBRs across Spain tripped offline rather than "riding through" the event and helping prevent cascading outages. As of October 1, 2026, NERC standards *PRC-029-1—Frequency and Voltage Ride-through Requirements for Inverter-based Resources* and *PRC-030-1—Unexpected Inverter-Based Resource Event Mitigation* will require US IBRs to have capabilities for ride-through and event mitigation.[64]

NERC requirements for dynamic voltage regulation and other reliability standards also protect the US grid from other contributors to the Iberian blackout.[65] Moreover, consistent with *PRC-024-3—Frequency and Voltage Protection Settings for Generating Resources,* operators set protections systems "such that generating resource(s) remain connected during defined frequency and voltage excursions."[66] These operators carefully seek to optimize the balance between protecting equipment while minimizing risks of unintended cascading trip-offs.

Nevertheless, three factors are intensifying the dangers posed by grid transformation—including cascading failures. The first lies in the growing complexity of the grid and the power flows across it. NERC's August 2025 *Reliability Risk Priorities Report* assesses the speed and breadth of these changes.

> Previously the grid had tens of thousands of devices under control, most of which were generation facilities. Grid frequency, energy balance, and stability were maintained by keeping those generation resources in tight synchrony with demand every few seconds. With increased penetration of generation, storage, and loads based on power electronics, the grid of the future will rely on millions of devices on both the transmission system and distribution systems to maintain reliability. Many of these devices will generally be smaller in size, more numerous, and geographically dispersed and include generation resources, energy storage facilities, and end-use loads, all of which may be asynchronous to the grid.[67]

This dispersed architecture is creating cascading risks beyond the regulatory reach of FERC and NERC. Millions of small-scale solar installations, batteries, and other distributed energy resources (DERs) are now feeding power into the BPS. NERC notes that "many of these devices on distribution systems will be controlled by common technologies, protocols, and network connections," which create risks of common failure modes and increase the scale of disruption that attacks can create. Moreover, many DERs are controlled by operators that are not subject to NERC's cyber standards, "which creates another risk vector."[68]

Surfing the Wave examined many of these dangers to reliability and proposed options to mitigate them. However, the 2025 NERC report identifies additional problems related to cascading outages.

64 Lauby, "Iberian Peninsula Blackout," 16. *PRC-029-1* will become effective October 1, 2026.

65 One especially valuable requirement in view of the Iberian outage: NERC VAR-002-4 and FERC Order 827 mandate that all generation units, including IBRs capable of voltage regulation, perform such control. Lauby, "Iberian Peninsula Blackout," 11.

66 NERC, *PRC-024-3*. In addition, as of October 1, 2026, enforcement of NERC, *PRC-024-4* will begin. Related standards already subject to enforcement include NERC, PRC-024-2; NERC, *PRC-026-2;* and others.

67 NERC, *2025 ERO Reliability Risk Priorities Report*, 36.

68 NERC, *2025 ERO Reliability Risk Priorities Report*, 37.

The deployment of advanced digitized equipment and increasingly automated control systems is accelerating. NERC notes that many such technologies "are yet unproven to operate in extreme conditions."[69] Deep interdependencies with other infrastructure sectors that adversaries may seek to disrupt (especially natural gas and communications industries) "are not fully understood."[70]

The expansion of power-hungry data centers creates additional risks for adversaries to exploit. In particular, NERC warns that rapid changes in demand from these loads will quickly "alter the flow of reactive power in the system, potentially exceeding the ability of existing voltage controls to respond and lead to over- and undervoltage conditions." Such conditions "could lead to the unplanned outages of generation plants initiated by voltage-ride through protection, load loss related to undervoltage load shedding, or even more widespread outages caused by voltage instability and collapse."[71] These risks will increase as new data centers require additional grid-provided power. As of 2025, US data centers consume approximately 4.4% of the nation's total electricity, a figure that some projections estimate will rise to between 6.7% and 12% by 2028.[72]

Crypto mining contributes to these risks, especially in ERCOT. Crypto mining facilities depend on constant, large-scale power supplies that are highly sensitive to voltage drops. When the voltage dips below a certain threshold, the computer "miners" shut down almost instantly, causing a rapid loss of load. NERC cautions that if such loads continue to grow in the ERCOT interconnection, "this load loss could grow to a level that would threaten the reliability of the Interconnection."[73]

Exacerbating all such problems: NERC finds that "industry lacks a comprehensive and systematic approach to incentivize resilience investments, and the costs required to significantly 'buy down' risk by hardening against high-impact but low-probability events are difficult to justify." Furthermore, the speed of the grid's transformation "further strains the timely implementation of such resilience investments."[74] The net effect: "Industry cannot keep pace with resilience threats."[75] That assessment makes it all the more important to strengthen defense in depth against cascading outages and improve our ability to sustain or rapidly restore electric service to critical loads when prevention measures fail.

Plan of the Study

- The next section of this report examines the grid's current fallback layers of defense to mitigate the effects of cascading failures.
- The third section explores how large, preplanned power islands could supplement these existing defenses and the circumstances in which islanding would make sense.
- The fourth section proposes how to leverage existing BA authorities and control areas to configure power islands and addresses a crucial problem with this option: the inability of islands to share power with each other to meet critical loads and limit the impact of PRC-induced disruptions.
- The fifth section analyzes options to separate islands from surrounding electric systems, either on condition (when emergency actions to prevent cascades begin to fail) or on intelligence and warning (when the president determines that potentially catastrophic attacks are imminent or underway).

69 NERC, *2025 ERO Reliability Risk Priorities Report*, 23.

70 NERC, *2025 ERO Reliability Risk Priorities Report*, 31.

71 NERC, *Characteristics and Risks*, 20.

72 Enriquez-Contreras et al., *MegaWatt Mayhem*, 10.

73 NERC, *Incident Review*, 1–2.

74 NERC, *2025 ERO Reliability Risk Priorities Report*, 24.

75 NERC, *2025 ERO Reliability Risk Priorities Report*, 17.

- The sixth section examines requirements to strengthen island resilience against attack.
- The seventh section recommends ways to maximize the deterrence benefits of islanding and—ideally—reduce the likelihood that islanding and other extreme and disruptive emergency measures will ever be necessary.
- The eighth section suggests options to overcome additional barriers to implementing strategic islanding, including the need to indemnify grid operators against the near certainty that island separation will cause economic losses and deaths to customers within those islands.

Current Fallback Defenses

If load shedding and other emergency actions fail to halt the spread of PRC-induced instabilities and cascading failures create interconnection-wide blackouts, reliability coordinators (RCs) and other grid operators have two basic options to mitigate outage impacts. The ultimate fallback is to restart the grid from within blacked-out regions of the United States—supplemented, if possible, with power imported from adjacent electric systems that are still functioning. Another option is to attempt to stabilize and operate the unintended islands that will emerge during the uncontrolled separation of the grid.[76] Neither option can ensure that hospitals, water utilities, military bases, and other essential customers will have the power they need during PRC attacks.

Microgrids can sustain service to these customers. However, because of the new generators and other infrastructure they require, the United States will never be able to build enough of them to serve the thousands of critical loads necessary for national defense and public health and safety. Large-scale strategic power islands that rely on existing infrastructure could offer a more efficient option to power these facilities in a blackout and—potentially—provide other significant benefits as well.

Blackstart

TOPs and their partners typically restore power from the "outside in" by bringing electricity into a blacked-out region from unaffected surrounding areas. However, if adversaries can create and extend cascading failures across entire interconnections, TOPs are prepared to restart the grid from within the blacked-out area—i.e., "blackstart"—while also importing power if possible from any contiguous areas where high-voltage systems are still functioning.[77]

Blackstart suffers from major liabilities. One is the length of time required to complete the restoration process. Precisely estimating the time needed to restore service across an interconnection is impossible; the United States has never done so in the Texas, Western, or Eastern interconnection. Nevertheless, the "near miss" in Texas in February 2021 highlights the severity of the problem. Severe cold disrupted so many natural gas wells, pipelines, and gas-fired generators across the state that the Texas interconnection nearly suffered a total blackout. Bill Magness, then the CEO of ERCOT (which is the independent system operator, or ISO, for the interconnection), estimated that had such a blackout occurred, "it could be weeks" before power could be restored state-wide, "and depending on

[76] Remedial action schemes (RAS) provide more fully planned options for island separation and operation. As discussed later in this section, RAS could provide a basis for establishing strategic power islands in the Florida peninsula and other US regions.

[77] Spanish and Portuguese grid operators executed combined "inside out" and "outside in" restoration operations during the Iberian Peninsula blackout. ICS Investigation Expert Panel, *Final Report*, 25, 336. In some US regions, the ability of operators to import power from adjacent interconnections will be constrained by the limited availability of high-transmission interties between them. Simeone and Rose, *Barriers and Opportunities.*

the conditions you're operating under when you go into a black start condition, it could take longer than that."[78]

Magness also testified to Congress that given those restoration timelines, the "costs of restoration of the system, the economic loss to Texas, and the personal costs to the wellbeing of Texas citizens would be unfathomable."[79] Texas is far smaller than the Eastern and Western interconnections. Many more weeks would be required to restore them via blackstart, and disruption to critical defense and nondefense loads would be more severe.

The fact that utilities have never used blackstart to restore power in the continental United States constitutes a liability.

Another problem with relying on blackstart as our fallback against interconnection-wide outages lies in the fragility of the process and the power islands it creates. TOPs initiate restoration by starting up a "blackstart resource" (often hydropower or a small diesel generator) and sending the power it produces down an electrically isolated corridor (or "cranking path") to start up additional generators.[80] TOPs keep the resulting power island stable by picking up load to balance the increasing generation within it. Operators then bring more generators online to grow the power island and, with the help of RCs and other partners, synchronize the island with neighboring ones and ultimately reestablish the interconnection.

The initial islands formed under this process will be vulnerable to collapse. In particular, these islands will typically be in a fragile state because of the lack of adequate system inertia provided by synchronous generating units connected to the grid. As a result, disturbances could cause generating units (blackstart and other generating resources) to trip off and force a restart of the restoration process.[81] Efforts to synchronize neighboring islands to enable their integration provides an additional challenge. Repeated attempts by Spanish grid operators to synchronize key islands failed.[82] Adversaries seeking to extend the duration of the outages they inflict will almost surely seek to exacerbate such problems. The net result: the blackstart restoration process, which would already require many weeks to complete, could repeatedly break down and further delay the delivery of grid-provided power to critical facilities and functions.

There are good reasons why blackstart has never been employed in the continental United States. Even when cascading failures have blacked out entire regions, as in the August 14, 2003, Midwest, Northeast, and Ontario Canada outage, many customers got their service back within hours, though some areas waited two days or more.[83] A crucial enabler for that process: because so much of the interconnection was unaffected, operators were able to import power from surrounding systems to

[78] Buchele and Largey, "If the Texas Power Grid Had Gone Down."

[79] *Power Struggle*, 2.

[80] NERC defines a blackstart resource as "a generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for Real and Reactive Power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." NERC, *Glossary of Terms*, 7. The broader blackstart restoration process and the NERC standards that support it are described in FERC, *Blackstart and Next-Start Resource Availability*, 13. For additional details on blackstart process, see Stockton et al., *Electric Infrastructure Protection (EPRO) Handbook V.*

[81] FERC, *Blackstart and Next-Start Resource Availability*; and NERC, *Characteristics and Risks*, 36–37.

[82] ICS Investigation Expert Panel, *Final Report*, 351.

[83] In Detroit and other areas of Michigan, for example, over two million customers waited more than forty-eight hours for their power to be restored. Michigan Public Service Commission, *Report on the August 14th Blackout*, 13.

conduct "outside in" restoration instead of resorting to blackstart. External sources of power may also be available to obviate the need for blackstart (or supplement blackstart operations) in PRC-induced outages that cover only a few states.

However, when it comes to preparedness against interconnection-wide outages, the fact that utilities have never used blackstart to restore power in the continental United States constitutes a liability.[84] Utilities have built up immense expertise in conducting traditional outside-in restoration in response to hurricanes and other severe weather events. No remotely equivalent "real world" experience has helped grid operators strengthen their ability to perform blackstart. NERC's *EOP-005-3—System Restoration from Blackstart* and other standards provide an extensive array of requirements for planning, system capabilities, exercises, training, and coordination of restoration operations.[85] TOPs and their partners also use M&S tools and other means to strengthen their ability to adaptively plan and execute blackstart contingency operations if adversaries disable their primary cranking paths.

Nevertheless, the problem remains: utilities will need to effectively perform blackstart *the very first time* they attempt to do so, potentially in the face of sustained PRC attacks on restoration assets and supporting infrastructure (including natural gas supplies for generators).

The electric industry is exploring advanced technologies to strengthen blackstart system resilience and shorten the multiweek process that would likely be required to complete the restoration. The most promising technical option is to employ widely distributed batteries with grid-forming (GFM) inverters to help restart the grid. That option would complicate adversary targeting and attack requirements and might accelerate restoration by bringing power resources closer to priority loads.[86]

However, TOPs and their partners would need to resolve major problems before GFM-based blackstart could become practical, including the question of how grid operators will balance load with generation as they create and grow power islands.[87] And while vendors have been selling GFM batteries for years, a 2025 industry survey found that US deployments of them are lagging far behind projected levels.[88] Any benefits of GFM technologies for accelerated blackstart are years away at best.

Islands Will Happen Anyway, So Why Not Plan for Them?

While cascading outages can black out extraordinarily large regions, the cascading process almost always creates unintended electrical islands when portions of an interconnection undergo "uncontrolled separation." Such separation constitutes the unintended islanding of a portion of an electric system that includes generation or load and is typically caused by the operation of protection or control systems when the grid is experiencing severe instabilities.[89] In rare cases, unintended islands can

[84] Blackstart restoration has occurred in Puerto Rico and the Hawaiian Islands, but the vastly greater scale and complexity of blackstarting the three US interconnections limits the value of these island events for building continental preparedness, as does the absence of the cyber and physical attacks in those restoration events. DOE's Liberty Eclipse exercise program provides a test bed for utilities and their partners to practice contested restoration in a controlled and more realistic context. DOE, "Practicing Defense and Resilience."

[85] NERC, *EOP-005-3*; and *NERC, EOP-006-3*.

[86] Stockton et al., *Electric Infrastructure Protection (EPRO) Handbook V*.

[87] Stockton et al., *Electric Infrastructure Protection (EPRO) Handbook V*; and NERC, *White Paper*.

[88] Quint et al., *Call to Action*.

[89] Uncontrolled separation can be contributory or a result of instability or cascading (NERC, *Reliability Guideline,* 67–68). The unintended islands formed by uncontrolled separation differ from DER-related unintended islands, which are created when distributed generation resources continue to provide power to the portion of the grid to which they remain connected, potentially endangering restoration workers. Kroposki, "Prevention of Unintentional Islands."

prove quite durable even as surrounding systems black out. The sources of that durability offer valuable insights for planning strategic power islands that operators could segment from the grid before cascades breach their borders.

Many unplanned islands will be misaligned with existing BA areas for grid control, making it difficult to determine who should manage those islands and exacerbating the challenges of keeping them stable.

The 2003 blackout again provides a useful frame of reference. In the Eastern Interconnection (as well as ERCOT and the Western Interconnection), generators and loads operate at or very near a common sixty-hertz frequency. Under extreme losses of synchronism, interconnections can break apart into separate electrical islands; each island would begin to maintain its own frequency based on its load/generation balance.[90] That is exactly what happened as islands formed in 2003. As severe power swings spread from the Midwest to the Northeast, New York, Ontario, and New England separated from the rest of the Eastern Interconnection. Then, during the next three seconds, the islanded northern section of the Eastern Interconnection broke apart internally, forming multiple smaller islands.[91]

Severe imbalances between generation and load contributed to this uncontrolled separation and unintended islanding. Once the Northeast became isolated, it lost more and more generation relative to load as more and more power plants tripped offline to protect themselves from the growing disturbance. The severe swings in frequency and voltage in the area caused numerous lines to trip offline. Those trips caused the isolated area to break up into further and still smaller islands. The load/generation mismatch also affected voltages and frequency within these smaller areas, causing further generator trips and automatic underfrequency load shedding and leading to blackouts in many of those areas.[92]

Most of the resulting islands collapsed in minutes or less, with two significant exceptions:

- Much of New England as well as Canada's Maritime Provinces (New Brunswick and Nova Scotia) broke off as an island, and—just by luck—generation matched demand closely enough to keep the island operational.[93]
- An unintended island also formed in western New York that included the Niagara Falls power plant and other hydro resources, which also came into equilibrium with the island's load.[94]

These two islands stayed in operation out of sheer good fortune. The tripping off of transmission lines created them without any prior consideration of whether the load and generation within those islands was balanced. The vast majority of islands created in 2003 broke down in seconds or less because they lacked such an accidental balance. Moreover, a NERC study that examined unplanned islanding in severe events identified an additional problem: many unplanned islands will be misaligned with existing BA areas for grid control, making it difficult to determine who should

[90] US-Canada Power System Outage Task Force, *Final Report*, 8.

[91] US-Canada Power System Outage Task Force, *Final Report*, 90.

[92] US-Canada Power System Outage Task Force, *Final Report*, 100.

[93] US-Canada Power System Outage Task Force, *Final Report*, 90, 97–98, 103.

[94] US-Canada Power System Outage Task Force, *Final Report*, 100. Note that the Quebec system in Canada also survived power surges because that system is tied to the Eastern Interconnection via high-voltage direct current links rather than alternating current transmission lines, protecting Quebec from the power swings that cascaded across other regions. US-Canada Power System Outage Task Force, *Final Report*, 98, 102.

manage those islands and exacerbating the challenges of keeping them stable.[95]

BAs, RCs, and other BPS entities rigorously study where unintended islands are likely to form based on grid topology and other factors. Real-time digital simulators and other M&S tools can assist with these predictive efforts and help grid managers prepare for contingency operations to stabilize those islands and facilitate broader system restoration.[96] AI is enabling the development of increasingly sophisticated M&S tools to perform such contingency analysis.[97] Together with advances in EMS and sensors to help operators establish situational awareness and control over unintended islands, RCs and BAs are gaining capabilities to predict and manage such islands far more effectively than was possible in the 2003 blackout.

The Southwest Power Pool (SPP) exemplifies such preparedness efforts. The SPP Emergency Operating Plan directs that if outages create power islands, the SPP's BA should be prepared to identify them and determine their boundaries, coordinate with TOPs and generator operators, and perform other island monitoring and control functions.[98]

Over the longer term, still more effective technologies and concepts of operation may emerge to help unintended islands sustain service to critical loads. The Electric Power Research Institute's SOLAr Critical Infrastructure Energization (SOLACE) project constitutes an especially far-reaching initiative. This project developed automated ways to form emergency "energy pathways" that connect existing DERs with critical loads and to create power islands separated from surrounding electric systems to help protect them from disruptions.[99] As with GFM-enabled blackstart, however, any such solutions to mitigate the effects of wide-area blackouts are years away.

The use of advanced M&S tools, sensor technologies, and EMS capabilities to anticipate where uncontrolled separation is likely to create islands offers more immediate benefits. Nevertheless, such unintended islands will always involve risks of generation–load imbalances and the resulting uncertainties around serving critical loads. An alternative approach: *preplan* to create islands in future emergencies and draw their boundaries in advance to maximize their stability.

Microgrids

Microgrids constitute the most familiar type of preplanned power island and (along with stand-alone emergency generators) are the best available solution to the problem of sustaining electric service to critical facilities during blackouts. DOE's National Laboratory of the Rockies (formerly known as the National Renewable Energy Laboratory, or NREL) defines microgrids as "a group of interconnected loads and distributed energy resources that acts as a single controllable entity with respect to the grid."[100] Microgrids operate during normal conditions in a grid-connected mode, with power flowing to facilities within their boundaries from external generation, transmission, and distribution infrastructure. When blackouts are imminent or underway, managers of microgrids can disconnect them from the grid and employ their own generation and distribution systems to serve their loads.

Microgrids provide an excellent option to strengthen power resilience for water and wastewater utilities, military bases, and other critical facilities in short-duration power outages. As demonstrated

95 NERC, *Severe Impact Resilience*, 18–21.

96 Wang et al., "Dynamic Study of Dominion's System Restoration Plan."

97 Chen et al., *Artificial Intelligence/Machine Learning Technology*, 29–31.

98 SPP, *SPP BA Emergency Operating Plan V10*, 39.

99 EPRI, *SOLAr Critical Infrastructure Energization (SOLACE)*, 2-1.

100 Booth et al., *Microgrids for Energy Resilience*.

during California's August 2020 extreme heat wave, when the California Energy Commission coordinated with the US Navy and Marine Corps to activate several installation microgrids, significant experience already exists to conduct such segmentation in the event of an attack.[101]

Nevertheless, if cascading failures create interconnection-wide blackouts and blackstart restoration becomes necessary to reconnect these facilities with grid-provided power, microgrids will suffer from a number of failings.

Shortfalls in Emergency Fuel Supplies

A growing number of recently deployed microgrids are powered by hybrid plants that combine large solar photovoltaic arrays and battery energy storage systems (BESS). However, when separated from the grid, many other microgrids use generators fueled by diesel, with a smaller number of systems employing natural gas, propane, or gasoline. These diesel generators also offer a common source of emergency power for hospitals, nursing homes, police stations, cell towers, emergency operations centers, and many thousands of other users.

Even large microgrids usually depend on infrastructure and support functions that lie beyond their perimeters.

Multimegawatt water utilities and other installations with diesel-powered microgrids will face serious fuel supply problems in extended outages. Some water systems store enough diesel fuel on-site to operate for seven to nine days without resupply.[102] However, many other facilities can operate for only a few days with on-site fuel, in part because of state and local environmental regulations that constrain storage amounts. In a long-duration blackout, the generators in those microgrids will need to be resupplied.

In such an event, an enormous mismatch will emerge between the demand for fuel and the capacity of delivery fleets to provide it given the large number of facility owners that will be requesting resupply. No data exists on the ability of diesel fuel delivery fleets to simultaneously serve all such customers in their service areas. But it seems reasonable to assume that few if any fleets are sized to do so.[103] Moreover, these fuel trucks will need to navigate in a severely disrupted environment. In an interconnection-wide outage, the loss of electric service to traffic lights and other road infrastructure will create massive traffic jams in many regions. Adversaries can also attack such infrastructure to further impede deliveries. The US Department of Transportation issued an alert in August 2025 that an unnamed country had embedded undocumented cellular radios in batteries that power a wide range of US highway infrastructure and that such compromises could be used to create simultaneous outages.[104]

Inadequate Microgrid Size

As noted above, microgrids constructed over the last few years increasingly rely on hybrid solar/battery storage power plants, especially microgrids on large military bases and other installations that have ample space for solar arrays. These microgrids will be invulnerable to fuel resupply issues, as will future microgrids that employ small, modular nuclear reactors, microreactors, or enhanced geothermal generation.

However, even large microgrids usually depend on infrastructure and support functions that lie beyond their perimeters. Defense installations provide a case in point. Most military bases depend

101 CAISO, *Root Cause Analysis*, 67.

102 EPA, *Power Resilience*, 4-1.

103 Stockton, *Electric Infrastructure Protection (EPRO) Handbook II,* 158–171.

104 Winter and Satter, "Exclusive."

on their surrounding communities for water and wastewater service, housing for base personnel and their families, and other critical support functions. Microgrids will leave these functions vulnerable to disruption in wide-area blackouts. And while microgrids much larger than any existing today might conceivably be able to encompass all such supporting infrastructure, as well as co-located critical loads, constructing sufficient generation resources within the microgrid's perimeter will be enormously difficult.[105]

The problems associated with microgrid size are even more severe for the execution of DOW missions compared to those affecting individual installations. Deploying forces to and through US ports so they can "get to the fight" in East Asia exemplifies these mission assurance challenges.[106] The Defense Science Board (DSB) report on DOW's reliance on critical infrastructure notes that to project to conflicts abroad, the department is increasingly dependent on civilian infrastructure and support functions.

> Outsourcing of services (e.g., electricity, water, ground transportation) has been deemed more efficient, reliable, and cost effective for the Department. A similar model has been adopted by the service providers themselves, outsourcing many of their own support services and supplies to lower tier providers. As a result, [the Department] is dependent on increasingly fragile homeland infrastructure whose interdependencies are difficult to unravel, limiting visibility into infrastructure resiliency against intentional attacks or natural disasters.[107]

Building microgrids to sustain electric service to all of these critical nodes, and countering the PRC's goal of disrupting US force protection, would be a monumental and massively expensive task.

Cost

Microgrids almost always require new generation resources, distribution infrastructure, and control systems. The most comprehensive and frequently cited assessments of those costs are provided in a report by the DOE's National Laboratory of the Rockies.[108] The laboratory found that microgrid costs scale with the amount of power they need and with the type of microgrid being constructed. Microgrid costs per megawatt for community microgrids have the lowest average, at $2.1 million per megawatt. Commercial microgrids for industrial facilities and other uses have the highest average cost, at $4 million per megawatt, with college and hospital campuses falling in between.[109]

Medium-scale microgrids for industrial zones average about 50 megawatts, making their generator-only costs approximately $200 million for each installation.[110] However, many microgrids deployed over the past four years have capacities of 400 megawatts or more, with commensurately greater costs.[111]

Microgrids require other capital investments as well. BESS are vital for solar-powered microgrids. Other types of microgrids require BESS as well to ensure power quality, peak load shaving, and frequency regulation and to provide backup power. Microgrids also need EMS to control generation, monitor the system, and balance generation with

[105] Small modular reactors or significant numbers of microreactors may someday provide sufficient power for microgrids. Again, however, the anticipated cost of these reactors could prove prohibitive for many commercial microgrid developers.

[106] Busler, "The Fight to Get to the Fight."

[107] DOD DSB, *Department of Defense Dependencies*, 1.

[108] Formerly the NREL.

[109] Giraldez et al., *Phase I Microgrid Cost Study*; and DOE, *Microgrid Overview*, 7.

[110] No agreed-upon classification of microgrids yet exists. This assessment of medium-scale megawatt usage is provided by Uddin et al., "Microgrids," 10.

[111] C2ES, "*Microgrids*."

load when disturbances occur. Furthermore, they typically require the installation of additional distribution infrastructure and points of common coupling that allow microgrids to link, segment, and relink with the surrounding electric system.[112]

Multi-square-mile microgrids can have eye-popping costs that make them financially untenable.

Design costs constitute an additional expense and reflect a deeper problem for ramping up microgrid construction. Current microgrid projects are usually bespoke projects, custom designed for individual user needs and varying widely in their configurations and operations. This lack of standardization and the widely varying regulatory requirements from state to state drive higher costs, limiting scalability and slowing the microgrid deployment process.[113]

The result of all of these factors is that proposals for comprehensive, multi-square-mile microgrids can have eye-popping costs that make them financially untenable. For example, a project for Cleveland, Ohio, designed to provide resilient power for businesses, public institutions, and critical facilities in the city's downtown (comprising two to three square miles) came in at an estimated $100 million.[114] Needless to say, the microgrid was never built. DOW appropriations can help military bases get over such cost hurdles. The microgrid constructed by Schneider Electric for the Yokota Air Base in Japan, which enables the base to operate as a power island in future conflicts, cost $400 million.[115] Absent equivalent federal funding to support the build-out of microgrids, the capital spending they entail will continue to constrain their use as a defensive fallback against cascading failures.

Required Numbers for Nationwide Resilience

Approximately 700 microgrids are currently deployed in the United States and concentrated in Alaska, California, Georgia, Maryland, New York, Oklahoma, and Texas.[116] The number of facilities crucial for public safety is vastly greater. Water utilities exemplify the difficulty of building enough microgrids to power such vital facilities in interconnection-wide blackouts. There are over 148,000 public water systems in the United States.[117] Many of them are small, including those that serve hospitals with water systems. Others are immense. DC Water, for example, serves 725 square miles in the District of Columbia and parts of adjacent counties, with pumping stations, SCADA systems, and other electricity-dependent infrastructure embedded across that territory.[118]

Most large water and wastewater systems are equipped with diesel-fueled emergency power generators to sustain the operation of pumping stations and other essential facilities during blackouts. These generators are an essential contributor to resilience in normal-duration events. However, as noted above, an interconnection-wide outage could require these generators to operate for weeks until the blackstart restoration process reaches them. Refueling these generators in the midst of a blackout would be a monumental task. Moreover, constructing microgrids to serve even a small fraction of the 148,000 US water systems would be prohibitively expensive. Building microgrids for all

[112] Points of common coupling include circuit breakers, protective relays, and synchronization equipment that facilitate the connection, power exchange, control, and protection of power flows between the microgrid and the surrounding electric system. Uddin et al., "Microgrids," 5.

[113] C2ES, "Microgrids"; and Meissner, "AI and Microgrids."

[114] Burger, "$100 Million Microgrid."

[115] Hitchens, "Yokota Air Base."

[116] C2ES, "Microgrids."

[117] EPA, "Information about Public Water Systems."

[118] DC Water, *Approved FY 2024 Budgets.*

the other facilities essential for public health and safety, the economy, and national defense would be still more costly. Microgrids can never offer more than a niche solution to serve critical loads during interconnection-wide outages.

Regional Resilience Districts as an Alternative to Traditional Microgrids

Former DOW officials Franklin Kramer, Robert Bulter, and Melanie Teplinsky have proposed an initiative that would remedy major shortfalls of microgrids. As part of a broader effort to defend US infrastructure from Volt Typhoon and other attack vectors, these researchers recommend the creation of regional resilience districts around critical commercial and defense hubs.[119] Unlike traditional microgrids, resilience districts could be large enough to encompass all the interdependent infrastructure systems necessary to support key military bases, civilian seaports, and other facilities and functions that the PRC will seek to disrupt by cutting off their power.

The Norfolk region exemplifies the potential benefits of such an approach. With multiple US Navy and Air Force installations in the area, as well as the water utilities and other supporting systems on which their personnel and operations depend, it would be far more efficient to create a regional power island to sustain service to all of them rather than separate microgrids. The same would be true for the Houston Shipping Channel, the ports of Los Angeles and Long Beach, and other regions vital to US security. CISA's Regional Resiliency Assessment Program is already supporting planning initiatives in many such areas.[120]

However, separating regional resilience districts from the grid would entail formidable problems of grid control, topography, and emergency authorities. It would be enormously difficult to open all of the breakers in eastern Virginia necessary to isolate the Norfolk region. Nor is it likely that sufficient generation capacity would exist in that district to serve even the most critical loads within it. And who would have authority to operate the region's electric system? A better approach: take advantage of existing BA authorities, boundaries, and expertise to configure and operate large-scale power islands to secure critical load against cascading failures.

Strategic Power Islanding: Quandaries and Potential Benefits

Transmission system managers interviewed for this study emphasized that interconnections offer enormous benefits for resilience and that separating the grid into smaller islands would "throw these advantages out the window." One operator noted that "you always want as many interconnected systems as possible for resilience. Islanding goes totally against that!" Another stated that the ability of systems to import and export power within their interconnections is a vital and frequently used tool for managing disruptions of transmission lines and generation resources caused by natural hazards—and potentially, by cyber and physical attacks. The net assessment by these experts: "maintaining the integrity of the interconnections is much better for reliability than breaking them into islands."[121]

Current energy policy and regulatory initiatives are pushing for *more* transmission system connectivity within and between interconnections rather than recommending islands as an emergency defense. Studies by NERC and academic researchers call for a significant increase in electric transmission transfer capabilities to enhance reliability.[122] DOE's Sep-

119 Kramer et al., "Defeating the Cyber Invasion," 8.

120 CISA, "Regional Resiliency Assessment Program."

121 Interviews by the author with TOPs in the Eastern Interconnection who requested anonymity.

122 NERC, *Interregional Transfer Capability Study*, viii, xiii; Dizikes, "What's the Best Way to Expand?"; and Senga et al., "Implications of Policy-Driven Transmission Expansion."

tember 2025 Speed to Power initiative will expand generation and transmission infrastructure nationwide to meet growing electricity demand and help manage severe weather events.[123] And while impediments remain to transmission system expansion, FERC Order 2023 and other regulatory initiatives are facilitating growth, as will DOE's National Interest Electric Transmission Corridor Designation Process.[124]

What these efforts overlook is the danger that increased connectivity will become an attack vector and give the PRC a uniquely efficient means to disrupt critical loads across the United States. The electric industry and its government partners should build additional transmission systems as rapidly as possible to move power where it is needed and maximize the grid's efficiency. But if uncontrolled outages begin to spread across the interconnections, we will need more than blackstart and traditional microgrids to keep vital civilian and military facilities operating.

The section Island Separation in Grid Security Emergencies examines the conditions under which it would make sense to "pull the plug" and fall back from defending the interconnections to separating them into strategic power islands. First, however, it will be helpful to analyze the pitfalls and potential benefits of islanding.

Lessons of 1965

While the massive 2003 blackout in the United States and Canada created multiple (and mostly short-lived) unintended power islands, a more useful case study for intentional islanding lies in the November 9, 1965, Northeast outage that propagated across all of New York state, portions of seven nearby states, and parts of eastern Canada. The 1965 cascading process is typical of such events. When a protective relay on an Ontario transmission line tripped, several other heavily loaded lines failed in rapid succession. The resulting surge of power overwhelmed the transmission lines in western New York, causing the cascading trips across additional lines and the eventual breakup of the entire Northeastern transmission network.[125]

Despite the speed of these cascades, which took ten minutes from start to finish, operators of the Long Island Lighting Company saw an opportunity to separate their electric system from Consolidated Edison (ConEd) in New York and prevent failures from spreading to the island's grid. Those operators severed the system's tie with ConEd in what the Federal Power Commission termed "a fruitless effort to save itself." Long Island's move also halted the flow of the power it had been sending to ConEd, creating further problems for the latter.[126]

The commission's assessment of such intentional islanding resonates today. The commission found that "the whole concept of the interconnected system depends upon mutual support in time of trouble" and that "a system operator should not be overly quick to separate" in emergencies "since it may be possible to hold the system together." Moreover, the criteria under which connected systems "will abandon mutual assistance and try to save themselves must be coordinated throughout the group."[127]

Sixty years later, those findings remain compelling. The choice faced by Long Island operators was whether to continue assisting their neighbors to defend the grid against intensifying voltage drops and other instabilities or to abandon that effort to

123 DOE, "Speed to Power." On the analytic and policy rational for this effort and for expanding transmission systems and generation resources across the United States, see DOE, *Resource Adequacy Report.*

124 FERC, *Improvements to Generator Interconnection*; and DOE, "National Interest Electric Transmission Corridor Designation."

125 Federal Power Commission, *Northeast Power Failure*, 14–17.

126 Federal Power Commission, *Northeast Power Failure*, 14.

127 Federal Power Commission, *Northeast Power Failure,* 16–17.

save their own system. ConEd had a similar choice. Its operators decided *not* to separate from the rest of the New York State system, even though ConEd was exporting power to that system and (in retrospect) might have survived had it islanded.

In contrast to microgrids, which require the construction of new generation resources, BESS, distribution lines, and other infrastructure, strategic power islands would utilize the existing assets within their boundaries.

Operators of strategic power islands will face equivalent, and equally difficult, decisions. However, as the commission stated, islands should not be too quick to abandon interconnected operations. Criteria for separation should delay islanding as long as possible and maximize opportunities for emergency actions and mutual support to stave off cascades. Close coordination and preplanning between neighboring systems will also be crucial to minimizing the disruptive effects of halting power flows between them. The decision criteria proposed in the section Island Separation in Grid Security Emergencies address all of these requirements.

As with all previous cascades, however, adversary attacks played no role in creating the 1965 blackout or in disrupting the Long Island system's attempt to "save its own skin." Future islands will not be so lucky. In tandem with PRC analysis of how to create cascading failures in the Western interconnection and elsewhere, Chinese researchers are also examining the challenges of separating islands from the grid and keeping them stable.[128] If China assesses that strategic power islands can sustain the service to critical loads that their cascading outages would otherwise disrupt, islands and their electric infrastructure will become prime targets of attack. Requirements to defeat such targeted strikes will add to the already formidable problems of island planning and operation. Yet, if islands are sufficiently resilient, they could offer unique national security benefits in wartime.

The Value Proposition

Strategic power islands would differ from the dozens of "steady state" power islands already in operation in the United States in Puerto Rico, the Hawaiian Islands, Guam, and multiple Alaskan islands. These existing power islands are not connected to the continental US BPS and function independently from it. However, these islands are in constant operation. Strategic power islands would only segment from the grid if cascading failures were imminent or underway and would otherwise stay integrated with the BPS to benefit from the peacetime resilience that the interconnections provide. Defining characteristics and potential advantages of such islands are discussed in the following subsections.

Reliance on Existing Grid Infrastructure

In contrast to microgrids, which require the construction of new generation resources, BESS, distribution lines, and other infrastructure, strategic power islands would utilize the existing assets within their boundaries. These islands would also leverage the ongoing build-out of thermal generators (primarily natural gas) and the expanded operation of coal plants under Trump administration policies, as well as existing hydro, geothermal, and solar resources and—eventually—advanced nuclear reactors.[129] In addition to the cost savings associated with relying on existing versus new infrastructure, employing these generation resources would

[128] Tang et al., "Intentional Controlled Islanding Strategy."

[129] DOE, "Energy Department Announces $625 Million Investment."

free power islands from depending on fuel resupply for diesel generators.[130]

Advantages of Scale

Only a relative handful of multistate power islands will be required to sustain service to critical customers nationwide compared with the many thousands of microgrids that would be required to provide equivalent coverage. These islands will also be sufficiently large to ensure that interdependent water, communications, financial services, and other infrastructure facilities are part of a shared power resilience footprint.

The potential advantages for contested DOW force protection are especially compelling. Given the complex web of civilian infrastructure and support functions necessary to enable force projection from bases deep inside the United States to and through US ports, strategic power islands could offer a uniquely efficient way to counter PRC goals in attacking the grid.

Redundant Electric Infrastructure

One of the advantages of interconnections (especially the Eastern and Western) is that they contain redundant generators, transmission systems, and other assets so that if one is disrupted, grid managers can use other assets to sustain reliable service. Strategic power islands will not replicate those levels of redundancy but can and should be scaled up to meet the "N – 1 criterion" for reliable operation.

As FERC describes this criterion, the electric system must be able to remain in a secure condition following the unexpected loss of the most important generator or transmission facility (a "single largest contingency"). Use of this N – 1 criterion "means that the loss of the most important generator or transmission facility does not jeopardize the remaining facilities in the system by causing them to exceed their emergency ratings or stability limits, which could lead to a cascading outage."[131] The multistate strategic power islands proposed in the section Current Fallback Defenses will contain sufficient redundant infrastructure to meet this criterion.

Additional Reliability Benefits

Relying on large thermal generators and (wherever possible) hydro plants would also offer strategic power islands reliability benefits. In contrast to microgrids, the boundaries of multistate islands can be drawn to encompass many megawatts of base load and dispatchable generation. Base load generation is traditionally composed of large thermal units as well as hydro and nuclear plants that run almost continuously to serve a base level of demand due to everyday needs. Gas turbine generators are highly dispatchable to meet sudden increases in demand and (along with BESS) help island managers balance generation with load.

If separation prevents cascading blackouts and operators can mitigate cyber and physical attacks against island infrastructure, the United States may be able to greatly reduce the number of regions that require blackstart restoration.

This mix of large-scale generation will also help provide islands with system inertia far beyond the levels possible with microgrids. The large amounts of energy stored in rotating masses (such as the spinning turbines of generation plants) are resistant

[130] Adversaries may attack the supply of natural gas for gas-fired generators in power islands. The section Drawing the Boundaries of Strategic Power Islands addresses these challenges.

[131] FERC, *Reliability Primer,* 22. Note that electric system entities prefer to use the term "single critical" versus "most important" asset for N – 1 analysis.

to changes in rotational speed. The inertia resists a decline in speed caused by the disruption of a generator, allowing control systems a brief opportunity to automatically produce more power from the remaining generators.[132] These characteristics of system inertia will help island operators manage frequency disturbances that attackers will seek to create.

In addition, the scale of the islands and the resources they encompass will help BAs maintain contingency reserves to respond to the unexpected failure or outage of a system component, such as a generator, transmission line, or other electrical element.[133] Assuming that adversaries will attack the islands that survive cascading failures, such reserves (together with inertia and other island characteristics described in the sections on current fallback defenses and drawing the boundaries of strategic power islands) will then sustain service to critical customers even in long-duration outages.

Facilitate (and Reduce Requirements) for Power Restoration

If separation prevents cascading blackouts from disrupting the electric infrastructure within islands and their operators can mitigate cyber and physical attacks against island infrastructure, the United States may be able to greatly reduce the number of regions that require blackstart restoration. Given the many weeks that will probably be required to complete blackstart operations, such reductions would offer enormous benefits for defense mission execution and public health and safety.

Of course, given the risk that adversaries may black out even well-defended islands, operators will need plans and capabilities to conduct blackstart within them and take advantage of the hydro, fossil-fueled generators, and other sources of inertia within their boundaries to mitigate the potential instabilities of emerging blackstart islands (i.e., islands within the islands).

Strategic power islands may enable nuclear power plants to stay online even when surrounding areas suffer from cascading failures.

Islands can offer an additional benefit for nationwide power restoration. If some islands survive cascades and subsequent Chinese attacks while other islands black out, the survivors will be able to flow power to neighboring systems and help reenergize their generators and other infrastructure in a manner equivalent to traditional, "outside-in" restoration. Compared with the extended timelines for blackstart, using strategic power islands to facilitate restoration nationwide could be significantly faster.

A Stretch Goal: Keep Nuclear Power Plants Up and Running

Grid-provided electric service (or "off-site power") is essential to support nuclear power plant operations and safety during normal conditions. If severe transmission system instabilities occur, nuclear power plants separate from the grid and transition to safe shutdown, during which emergency power generators and batteries keep the reactors safe and power critical station loads.[134] Of course, this separation also means that plants are no longer delivering electricity to the grid.

Strategic power islands may enable nuclear power plants to stay online even when surrounding areas suffer from cascading failures. As long as transmission systems inside the island stay connected to those plants and the islands have sufficient load to accept their power output (along with other "always on" baseload generation resources), nuclear power might continue to serve critical customers rather

132 FERC, *Reliability Primer,* 14.

133 NERC, *Glossary of Terms*, 13–14.

134 Nuclear Regulatory Commission, "Station Blackout."

than automatically shutting down. Almost 20% of US electricity is generated by nuclear plants, which also provide inertia to help manage instabilities.[135] Nuclear plants are also specially hardened against cyber and kinetic attacks. Keeping electricity flowing from these plants would constitute an enormous advantage for strategic power islands.

An Even Taller Order: Bolster Deterrence of PRC Attacks

Chinese leaders have excellent reasons to doubt whether blackstart will be fast and effective enough to prevent the PRC from inducing societal panic, disrupting fort-to-port operations, and achieving its other goals in attacking the grid. These leaders may assess that US efforts to manage unintended islands "on the fly" are even less likely to succeed. If the United States can prepare instead to operate preplanned islands in future crises and sustain service to key military facilities (including those for responding to PRC attacks), Chinese leaders may lose confidence that they can achieve their objectives at an acceptable cost.

Building Blocks for Progress

This report is not the first to explore the possibility of creating large, preplanned islands for grid emergencies. A 2017 report by the National Academies of Sciences, Engineering, and Medicine offered a brief description of how "adaptive islanding" could enable preplanned islands to segment from the grid in emergencies.[136] DOE never acted on the report's recommendation to conduct further research on adaptive islanding.

Nevertheless, foundations are already in place to assist islanding initiatives. Dozens of power and electrical engineering studies analyze algorithms to help operators configure and manage "intentional controlled islanding." Some of these algorithms and their underlying methodologies can help operators take the next step: that is, leverage America's existing BA boundaries and authorities to bolster defense against adversary-induced cascades.[137] TOPs and their partners also have remedial action schemes to mitigate the consequences of extreme events. As discussed below, these schemes also offer useful data for designing and operating preplanned islands.

Differentiating Islands by Scale and Purpose

The National Laboratory of the Rockies[138] provides a useful typology of preplanned, intentional islands that can separate from the grid and function without external power sources. At the smallest scale, local electric power system (EPS) islands serve single facilities, including customer residences and commercial buildings. Larger microgrids covered by IEEE Standard 1547 and related documents constitute planned electrical islands "capable of being energized by one or more Local EPSs." NREL notes that BPS areas could be configured into much larger islands but that no equivalent IEEE design or operating standards exist for them.[139]

Creating large islands could serve two very different purposes. This study examines how strategic power islands can be separated from the grid to defend them from cascading failures and sustain service to critical loads within their boundaries.[140] Grid operators can also flip that model. If a portion of the BPS becomes dangerously unstable, operators can

[135] EIA, "What Is U.S. Electricity Generation by Energy Source?"

[136] NASEM, *Enhancing the Resilience of the Nation's Electricity System*.

[137] For a comprehensive review of power engineering literature on intentional controlled islanding, see Hassani Ahangar et al., "Review on Intentional Controlled Islanding."

[138] Formerly the NREL.

[139] Narang et al., *Overview of Functional Technical Requirements*, 1–4.

[140] EPRI offers a brief description of such islanding in EPRI, *Use Case 14*.

separate that area to stop the spread of instabilities to neighboring systems. A 2025 study examines the use of such "intentional system partitioning" as "a last-resort remedial action designed to confine cascading failures and limit blackout severity."[141] Or, as one former BPS regulator puts it, "islanding can help prevent the tail from wagging the dog off the cliff."[142] BPS entities should keep such an option in their emergency playbooks.

Remedial Action Schemes

Another playbook component bears more directly on strategic power islanding. Remedial action schemes (RAS) provide grid operators with a valuable way to "limit the impact of Cascading or extreme events." RAS are schemes "designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation (MW and Mvar), tripping load, or reconfiguring a System(s)."[143] A report by the Pacific Northwest National Laboratory (PNNL) notes that RAS are "used throughout the electric utility transmission systems" as a means to respond to abnormal or predetermined system conditions to maintain overall system reliability.[144] RAS that enable grid reconfiguration can provide especially useful data for planning strategic power islands.

Florida exemplifies such opportunities. The Florida Reliability Coordinating Council (FRCC), which is the RC for much of the state, has a RAS that triggers a controlled separation between peninsular Florida and the rest of the Eastern Interconnection during a severe event (including cascading failures). The separation points are at locations where relays can reliably detect conditions that merit separation.[145] Grid operators in the Western Interconnection and other regions have RAS as well, which can include actions to open interconnecting lines and establish emergency islands.[146]

The well-established, clearly defined boundaries of BA service areas and the control functions they perform offer ideal starting points for designing strategic power islands in many—though not all—US regions.

While the design of strategic power islands can draw on RAS in regions such as Florida, the next section explains why balancing authority areas (BAAs) will provide a better basis for island configuration in much of the United States. Nevertheless, NERC standards that apply to RAS include a requirement that must be broadly applied to plans for island separation. NERC warns that RAS actions "can have a significant impact on the reliability and integrity" of the BPS, including potentially destabilizing interactions among separate RAS and other protection and control systems. NERC's *PRC-012-2—Remedial Action Schemes* establishes requirements for grid operators to avert such problems and the instabilities they could create.[147] As discussed with regard to the 1965 blackout, options to separate strategic power islands from the grid will need to account for a similar danger that separation will destabilize neighboring systems and inadvertently magnify the effects of Chinese attacks.

141 Hashemi, "Cascading-Driven Intentional Controlled Islanding."

142 2025 interview with a source who prefers to stay anonymous.

143 NERC, *Glossary of Terms*, 35–37.

144 PNNL, "Transformative Remedial Action Scheme Tool."

145 NERC, *Reliability Guideline*, 69–70.

146 RFL, "Remedial Action Scheme." See also NERC, *PRC-012-2*.

147 NERC, *PRC-012-2*.

Drawing the Boundaries of Strategic Power Islands

The well-established, clearly defined boundaries of BA service areas and the control functions they perform offer ideal starting points for designing strategic power islands in many—though not all—US regions. Some BAAs contain so little generation and load that they would be inherently less stable than their larger counterparts. Other BAAs in California and elsewhere have ample load but need to import massive amounts of power from other regions to serve their customers. Still other BAs import (and, occasionally, export) power across the US–Canada border, creating requirements for binational coordination on islanding.

Electricity sharing also entails problems for island resilience. BAs routinely request power from adjacent BAAs to help them meet surges in demand, respond to the temporary loss of generation resources, and manage instabilities. When strategic power islands separate from the grid, such power exchanges will no longer be possible. Island operators will need to manage PRC-induced instabilities on their own.

To help them do so, it will be essential to aggregate small BAs into larger entities that contain greater generation and load. The very largest BAs will need to counter a different problem: the risk that cascading failures will occur within their boundaries. Moreover, for all BAs, the difficulties of meeting demand from generation resources within their boundaries will be exacerbated by a widening gap between supplies of US electricity and spiking demand for them.

"Hit the Easy Button": BAAs as the Starting Point for Island Design

According to April 2026 data from the US Energy Information Agency, there are sixty-four BAs operating in the United States.[148] The number and configuration of these BAs continue to evolve. On April 1, 2026, for example, SPP established the SPP West BAA to serve power companies in the Western Interconnection, supplementing SPP's existing BAA that provides balancing services to utilities in the Eastern Interconnection.[149] As will be discussed below, a number of small utilities that operate as independent BAs plan to integrate into larger ones. With the caveat that these changes are ongoing, Figure 1 displays the approximate locations of the sixty-four BAs within the three interconnections in the lower forty-eight states.[150]

Even the smallest BAs will be more durable than most of the unintended islands that cascading failure will create.

Almost all BAs are utilities, Power Marketing Administrations, or groups of utilities that have formed regional entities called regional transmission organizations (RTOs) and independent system operators (ISOs).

BAs are distributed across these interconnections as follows:

- The Eastern Interconnection encompasses the area east of the Rocky Mountains and a portion of northern Texas. The Eastern Interconnection

[148] EIA, "Hourly Electric Grid Monitor." Note that the EIA-930 reference table lists a total of seventy-two US BAs, but that eight of them have been retired since 2015. For example, according to the EIA, South Energy Cooperative (PowerSouth) relinquished its role as an independent BA on Sept. 1, 2021, entering into a Coordinated Planning and Operations agreement with Alabama Power/Southern Company.

[149] SPP, *2026 RTO Expansion*, 1.

[150] The boundaries for the SPP and SPP West BAAs are adapted from Waldoch, "SPP Expansion." Primary sources for the map and analysis in this section include FERC, Reliability Primer; DOE, "How It Works"; NERC, *Balancing and Frequency Control*; and EIA, "Hourly Electric Grid Monitor."

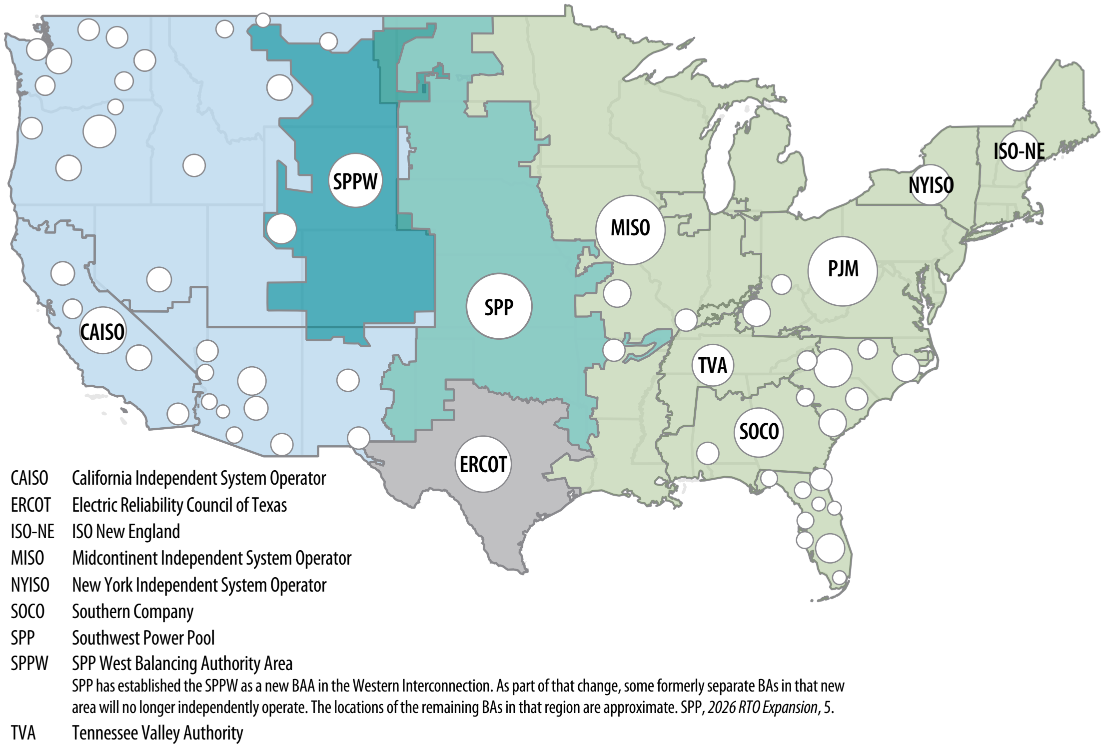

Figure 1. US Electric Power Regions

consists of approximately thirty BAs in the United States and an additional five in Canada.

- The Western Interconnection encompasses the area from the Rockies west and consists of approximately thirty-three BAs in the United States, two in Canada, and one in Mexico.
- The ERCOT covers most, but not all, of Texas and consists of a single BA.[151]

Each BA in an interconnection is connected via a small number of high-voltage transmission lines (called tie lines) to neighboring BAs. RCs oversee the BA operations and coordination. BAs are responsible for the supply/demand balance within their BAA, while RCs are responsible for the wide-area health of the interconnection.[152]

All US RTOs and ISOs serve as BAs.[153] Note that the ERCOT is unique in that the area's BA, interconnection, and the RTO are all the same entity and physical system. Many other BAs are electric utilities that have taken on the balancing responsibilities for specific areas of their interconnections—i.e., their BAAs.

The circles in Figure 1 display the approximate size of US BAAs (though not their actual boundaries). The Eastern Interconnection SPP, Midcontinent Independent System Operator (MISO), and PJM BAs are massive in geographic scope and in terms of the total generation and load within their boundaries. PJM, for example, served an estimated summer

151 EIA, *US Electric System.*

152 NERC, *Balancing and Frequency Control*, 2.

153 ISOs grew out of FERC Orders 888 and 889, in which the commission suggested the concept of an ISO as one way for existing tight power pools to satisfy the requirement of providing nondiscriminatory access to transmission. Subsequently, in Order 2000, the commission encouraged the voluntary formation of RTOs to administer the transmission grid on a regional basis throughout North America (including Canada). FERC, "RTOs and ISOs."

2024 peak load of approximately 151,000 megawatts.[154] Again, Figure 1 depicts only the approximate size of these BAAs. As in the case of SPP, which added utilities in seven states (Arizona, Colorado, Montana, Nebraska, New Mexico, Utah, and Wyoming) in March 2026, the exact boundaries of these areas are continuously evolving.[155]

Small BAs in Florida exemplify the other end of the spectrum. While Florida Power & Light (FPL) operates a large BA in terms of generation and load, a study by NREL found that many others are tiny in comparison, with the Gainesville Regional Utilities BA serving less than 2% of FPL's total load.[156] The Pacific Northwest and Arizona also include many small BAAs.[157]

Using BA Authorities, Functions, and Partnerships for Islanding

Even the smallest BAs will be more durable than most of the unintended islands that cascading failures will create. BAAs have fixed boundaries and are operated by personnel with deep familiarity with the electric infrastructure within them. Those personnel are also are experts in balancing generation and load inside their BAs. Accordingly, configuring islands around BAAs offers a far better option than relying on uncontrolled separation to produce survivable islands.

All of these BA advantages will be crucial for balancing operations in the face of PRC attacks. If disruptions of generation or transmission infrastructure sharply reduce power supplies, those reductions could cause a drop in frequency below the stable system frequency, risking significant permanent physical damage to electrical equipment and prolonged grid-wide blackouts. Moreover, as the frequency drops below safe operating levels, many generators will automatically disconnect from the grid for self-protection. As generators and other electrical equipment shut down, electricity supply will continue to decline, causing the system frequency to drop even further and—potentially—contributing to cascading failures.[158]

The expertise of BAs in conducting balancing makes them indispensable for preventing cascading outages in coordination with RCs, TOPs, and other grid partners. That same expertise will be crucial for keeping islands stable when they separate from the grid. NERC reliability standards for BAs, including requirements for gathering near-real-time data on potential grid-control problems, give BAs further tools they can apply to islanded operation.[159] Emergency-related standards provide additional foundations for resilient islanding. For example, if adversaries disrupt a BA's primary control center, NERC standard EOP-008-2 requires them to have the "backup functionality" (including monitoring, control, logging, and alarming) necessary to continue meeting their grid reliability mandates.[160]

BAs will also be able to build on their deep relationships with other BPS entities to prepare for and conduct island operations. Key partners include the following:

- **Reliability coordinators.** RCs have the highest level of authority with respect to the reliable operation of the power grid.[161] RCs maintain a wide-area view of the grid and have the operating tools, processes, and

154 PJM, "PJM Publishes 2024 Long-Term Load Forecast."

155 T&D World, "Southwest Power Pool."

156 NREL, *Absorbing the Sun.*

157 EIA, *US Electric System.*

158 DOE, "How It Works," 5.

159 NERC, *BAL-005-1.*

160 NERC, *EOP-008-2.*

161 Under NERC's full definition of RCs, an RC is "the entity that is the highest level of authority who is responsible for the Reliable Operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations." NERC, *Glossary of Terms*, 42.

procedures—including the authority to prevent or mitigate emergency operating situations—needed for both next-day analysis and real-time operations. RCs are therefore crucial for preventing cascading failures and responding to them if they occur—including, potentially, supporting islanded operations. As will be discussed in the next section, these island roles will be especially prominent for PJM, MISO, and other grid operators that perform both RC and BA functions.

- **Transmission operators.** TOPs are responsible for the reliability of their "local" transmission systems and operate or direct the operations of the transmission facilities in their areas. While some entities both own and operate transmission assets, others do not. Transmission operators that do not own the transmission facilities have agreements with the owners to coordinate and operate those facilities. As with RCs, TOPs will play vital roles in implementing emergency actions to prevent cascades, and—if islands must separate when attacks are imminent or underway—coordinating with BAs to operate their local transmission systems within those islands.
- **Generator operators.** GOs operate supply electricity and provide additional services for reliable interconnected operations. While some entities both own and operate generation assets, this is not always the case. GOs that do not own the generating facilities have agreements with the owners to coordinate and operate those facilities. BAs collaborate closely with GOs to perform balancing in steady-state and emergency conditions. Those same relationships will be crucial for islanded operations.
- **Distribution providers.** DPs operate the "wires" between the transmission system and the end-use customer. Once BAAs separate from the grid, the resilience of DP systems will be essential for islands to serve critical defense and civilian loads.[162]

None of the NERC reliability standards that apply to BAs, RCs, and their BPS partners specifically authorize them to help separate the interconnections into islands. *TOP-001-6—Transmission Operations* seeks to "prevent instability, uncontrolled separation, or Cascading outages" by requiring "prompt action to prevent or mitigate such occurrences." That standard also states that "each Balancing Authority shall act to maintain the reliability of its Balancing Authority Area via its own actions or by issuing Operating Instructions."[163] Together with the authorities of RCs, with whom BAs will closely coordinate, these functions enable far-reaching emergency actions. Nothing in FERC or NERC regulations requires BAs or RCs to island the grid when doing so is consistent with their responsibilities—but nothing forbids them from doing so when cascading failures are imminent or underway.

Aggregating BAAs for Island Stability

Even with the close collaboration of all these partners, islands configured around small BAAs will be inherently less survivable than their large, multistate counterparts. Small islands would contain far less redundant infrastructure, system inertia, and contingency reserves than those based on the boundaries of MISO or other vast BAAs. A preferable strategy for resilience will be to combine multiple small BAAs into much larger, aggregated islands and drastically increase the amount of generation and load within their boundaries. The section that follows proposes specific options for aggregation in Florida and other US regions and recommends how RCs might help existing BA personnel manage these larger islands. Aggregation will not be possible for the small, geographically separated utilities that help provide power in

162 FERC, *Reliability Primer*, 27–28.

163 NERC, *TOP-001-6*, 1.

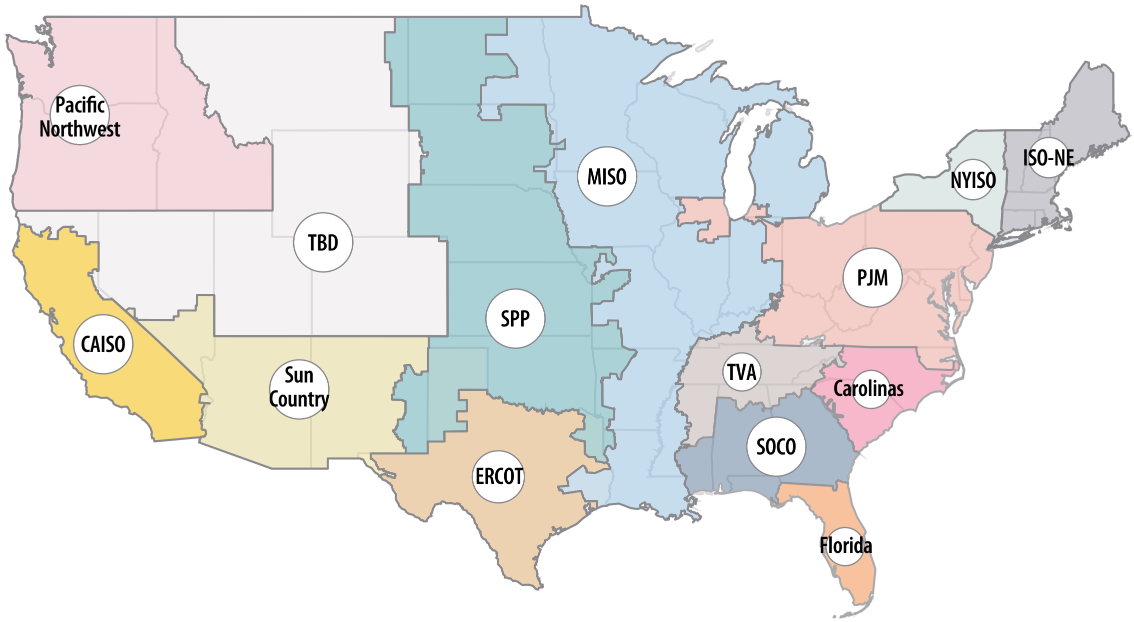

Figure 2. Proposed Strategic Power Island Boundaries

Alaska and Hawaii, whose military bases will make them prime targets for PRC attacks. Alaska's grid is fragmented into over 100 independent utilities and 150 microgrids.[164] The Railbelt Reliability Council is the state's electric reliability organization and oversees reliability for the utilities that serve most Alaskan customers.[165] In Hawaii, the electric reliability administrator oversees grid operations and cybersecurity efforts of the isolated electric systems that operate on each of the state's islands.[166] Aggregation strategies are not topographically feasible for many of these unconnected systems. Instead, continued investments in emergency power, microgrid construction, and infrastructure resilience will be necessary to strengthen energy resilience for critical defense installations and civilian facilities.[167]

A First Cut at Strategic Island Boundaries

Figure 2 recommends boundaries for US strategic power islands that reflect the existing borders of large BAs as well as for aggregated islands that would consolidate small ones. Of course, electric industry entities are best positioned to finalize such boundaries in consultation with government leaders and regulators. The section Electricity Sharing and Island Design examines specific factors that should help guide that process. The islands proposed here represent only a starting point to help grid operators and their partners develop more refined, engineering-informed plans.

Consolidating BAs: Florida, the Pacific Northwest, and the Southwest

As noted above, small power islands have disadvantages for resilience. With ten separate BAAs in the Florida peninsula, the best way to create a stable strategic power island in that region would be to combine those areas into a single entity and thereby greatly increase the aggregate generation, load, and system inertia within the new island.

164 IARC, "Alaska's Arctic Energy System."

165 RRC, "About the RRC."

166 State of Hawaii Public Utilities Commission, "Resilience and Reliability."

167 Similar approaches will be appropriate for Guam, Puerto Rico, and other US territorial islands. DOE GDO, *Territory of Guam*; and Clark, *Electric Reliability and Resiliency.*

Figure 2 illustrates how the region's grid operators and government officials might consolidate BAAs into a power island serving the Florida peninsula. The western Panhandle would remain in the island that would be based on the existing BAA of SOCO (Southern Company). Such plans could leverage the existing Florida RAS discussed in the section Strategic Power Islanding: Quandaries and Potential Benefits.

Figure 2 proposes similar consolidation initiatives for the Carolinas, the Pacific Northwest, and "Sun Country" (which would aggregate multiple small BAAs in Arizona and portions of New Mexico and Nevada). Grid managers and their partners will need to further analyze the area designated TBD in the Mountain West to optimize island design.

It is important to reiterate that these strategic power islands would join together and segment from the grid only if federal leaders determined that a potentially catastrophic attack were imminent or underway. During normal conditions, BAs would continue to control their areas just as they do today. A former manager of a small BA emphasized that "there is no chance that BAs will be willing to alter their boundaries" unless a dire emergency occurs. BAs are "jealous of their autonomy." During peacetime, mayors, county executives, and other local officials will continue to support existing BAA boundaries "regardless of political party."

However, the same BA manager stated that neighboring BAs in their region routinely conduct collaborative emergency exercises under the leadership of their RC. Some exercise activities, including cross-border power sharing between BAs, could also facilitate balancing if the BAs were consolidated into a single island. Other exercise activities involved building shared situational awareness of local grid conditions and coordinating emergency response actions. Again, all of these activities would help managers operate a consolidated island.

The desire by small BA managers to further strengthen their resilience is also helping drive some of them to take the next step: integration into larger islands. Despite the long-standing preference of these BAs to retain their autonomy, a growing number are now exploring integration options. The Rocky Mountain region of the Western Interconnection exemplifies these trends. Chris Hansen, CEO of the La Plata Electric Association in Colorado, notes that his utility's decision to join SPP "reflects a broader evolution underway across the Western grid. Utilities are moving away from localized operating models and toward more coordinated, regional approaches to managing electricity systems," including for balancing operations.[168] Improved reliability and resilience are not the only factors driving this transition. Greater efficiency in utilizing regional generation resources and other incentives are also encouraging small BAs to abandon their autonomy. Nevertheless, the shift toward integration will be extraordinarily helpful for strategic island design and operation.

For the small BAs that have not yet joined that trend, including those that serve critical defense installations, the next step in assessing integrated islanding options might be for those BAs and local government authorities to analyze how island boundaries could be configured to optimize balancing and reliability once separated from the grid. The BAs incorporated into such islands would also need to predetermine how to allocate authority over their emergency functions, with RCs, control staffs aggregated from multiple BAs, and coordination with TOPs and GOs all contributing to island management.

RC functions will offer special value for islanded operations. Every RC's area of responsibility coincides with one or more BAAs. In Florida, for example, the FRCC works closely with all ten peninsula BAs to help maintain the state grid's reliability and would coordinate with them on emergency response actions if cyberattacks were to occur. RCs such as the FRCC do not conduct balancing

[168] Hansen, "La Plata Electric CEO."

operations; that is the function of BAs. Nevertheless, other RC responsibilities (such as coordinating assistance between neighboring BAs and maintaining secure communications with all BAs and TOPs in an RC service area) would be helpful in managing consolidated power islands.[169]

BAs and other grid entities will not have sole authority to set island boundaries and determine who will operate them. Regulators and other officials at multiple levels of government will also want a say, especially since (as will be discussed later) emergency load shedding may be required to keep islands stable in a PRC attack. The leaders of consolidated, multi-BA power islands will also need to decide where and how to establish primary and backup control centers for combined islands, create communications protocols with unfamiliar GOs, and solve myriad other problems in the island design process.

Island Funding and Modeling

In contrast to microgrids, which require the construction of new generators and other infrastructure investments, strategic power islands would rely on existing infrastructure. That makes the latter option a more affordable way to serve critical loads across the United States. Nevertheless, strategic power islands would entail significant costs, including for the smaller BAs that have the fewest resources to pay for them.

M&S for island design and management constitutes one such expense. Large BAs already conduct extensive modeling efforts to predict where cascading failures could create unintended islands and build contingency plans to operate them. The same modeling capabilities will help BAs refine the boundaries of preplanned islands proposed in Figure 2 and account for anomalies in BAA service areas that have evolved over time.

PJM offers an example of how this process could go forward. The PJM island in Figure 2, which reflects PJM's existing territory, includes the Chicago region and a portion of southwest Michigan that is geographically separate from PJM's main service area. There might be advantages to assigning Chicago and southwest Michigan to the MISO island if emergency islanding becomes necessary. M&S tools and exercises can help determine whether that option makes sense in terms of grid topography and system management.

M&S will also be necessary to configure islands that aggregate small BAs. Island designers will need to identify the ties that will be opened, the locations of major generators and critical loads, and other preevent planning factors. Modeling can support such decision-making and optimize island boundaries. Once those boundaries are established, simulation tools can help train grid managers to operate the islands after they separate.

All such M&S initiatives will require funding. The investments required for M&S studies, emergency operations planning, training, and exercises will be far less than those needed to deploy new generators or meet other microgrid construction costs. PJM, MISO, and other very large BAs already possess advanced M&S capabilities and staffs trained to utilize them. That will not be true of the small BAs that will comprise aggregated islands. The Implementation section of this study proposes that Congress appropriate such funding because strategic power islands would directly support the common defense. But winning congressional approval for such funding constitutes yet another impediment to adopting strategic power islands as a line of defense against cascading failures.

Subdivide the "Whales" in Wartime?

BAs at the other end of the size spectrum from Gainesville, Florida, pose island design problems of a different sort. The proposed islands based on the existing BAA boundaries of ERCOT, MISO, PJM,

[169] NERC, *IRO-008-3*; and NERC, *IRO-002-7*.

and SPP footprints are massive. That scale offers advantages in terms of infrastructure redundancy and other factors that contribute to their resilience. But could they also be so large that the PRC could induce cascading failures across their territories and obviate the benefits of islanding?

PJM exemplifies the question of "how big is too big?" for island defense. As noted above, PJM's territory is enormous, serving thirteen states and the District of Columbia and sixty-seven million people with 182,000 megawatts of generation capacity and 88,333 miles of transmission lines.[170] That territory comprises a vast array of facilities and functions the PRC may seek to disrupt via power blackouts, from financial services sector infrastructure in New Jersey to the National Capitol Region and multiple Navy and Air Force installations in the Norfolk region.

In some strategically important US regions, BAAs (and islands based on them) will be in deep trouble if they can no longer import power from their neighbors.

PJM has terrific expertise in managing weather-induced disturbances in its BAA, and continuing to exercise centralized control over that area as a single, integrated power island offers significant advantages. But in especially severe events that stress PJM's span of control, it may be helpful to have contingency plans to segment the BA into two or more smaller islands. BAs that serve other very large areas, including MISO, SPP, and ERCOT, may want to develop contingency plans that reflect their own grid topologies, concentrations of multiple national security loads, and other factors.

The most important impetus for such planning lies in the potential vulnerability of very large islands to cascading failures. For context, it is useful to note that the three US interconnections already function as massive power islands, with very limited interties between them. Chinese researchers are examining how to create cascading blackouts within those interconnections. The PRC is sure to do the same for preplanned, multistate power islands.

Subdividing such islands might reduce their risks of internal cascades after separation, including through improved voltage control, by (1) ensuring adequacy of local reactive power supplies and (2) relying on nearby generation resources versus assets many hundreds of miles away, as well as avoiding large-scale transfers of such power over long-distance transmission lines with limited rights of way.[171] In addition, just as advanced M&S tools help grid managers identify where uncontrolled separation is likely to create unintended islands, these managers can also anticipate where their territories are likely to subdivide and preplan to operate those segments to hedge against cascading failures.

Yet, the size of these BAs offers advantages for regional resilience. The District of Columbia (DC) has dozens of power-hungry facilities that are vital for US security. The amount of generation capacity in DC is tiny compared with those loads. Indeed, the District consumes about eighty-three times more energy than it produces.[172] The electricity that powers DC comes from elsewhere in the PJM territory, including the energy-rich state of Pennsylvania. Breaking PJM up so that DC could become its own strategic power island would be wholly impractical. Electricity sharing across many other large BAAs offers equivalent advantages. But in some strategically important US regions, BAAs

170 PJM, "PJM – At a Glance."

171 For an example of how large transfers of energy over long distances with limited rights of way can contribute to cascading failures, including through the large amounts of remote generation that results in power and voltage swings on the system, see NWPCC, "Blackout of 1996." Note, in particular, how high north–south transfers contributed to cascades in that event.

172 EIA, "District of Columbia Analysis."

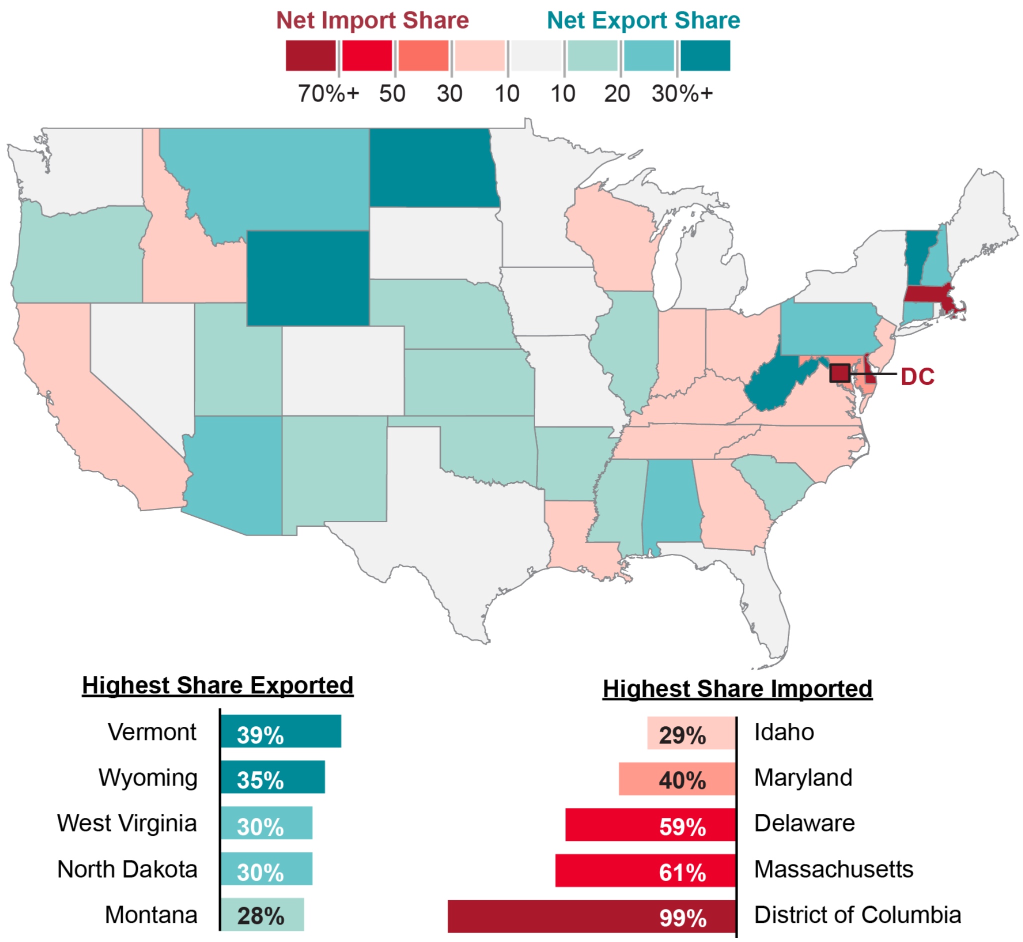

Figure 3. State Net Electricity Exports and Imports

(and islands based on them) will be in deep trouble if they can no longer import power from their neighbors.

Electricity Sharing and Island Design

The states that would comprise strategic power islands differ in terms of whether they are net importers or exporters of power. Some states (and DC) have far more load than they can serve with generation resources within their borders. Other states are major electricity producers but have few customers to consume their power. Still others import and, occasionally, export power across the US–Canada border. These power-sharing profiles have important implications for island configuration and resilience.

Figure 3 depicts how US states vary in how much power they import or export. As noted above, BAAs such as PJM routinely flow power from high-generation states to net importers. Those flows reflect the crucial role of interstate (and interregional) power sharing in the US grid—a role that is poised to grow under Trump administration policies and private-sector initiatives to expand the US high-voltage transmission system.

The US Energy Information Administration (EIA) notes that "electricity routinely flows between the lower 48 states." Electricity generation exceeds electricity consumption in twenty-five states, and excess electricity is transmitted across state lines—almost 10% of US electricity generation is traded among states.[173] As noted above, some large BAAs

[173] EIA, "California Was the Largest Net Electricity Importer."

and the power islands that would be based on them employ these cross-state power flows to meet the needs of DC and other major importers. Those flows would continue if such islands segment from the interconnections.

California is in a more difficult situation. The California Independent System Operator (CAISO) is the largest of about thirty-eight BAs in the Western Interconnection, handling an estimated 35% of the electric load in the West and covering much (though not all) of the state's territory.[174] As depicted in Figure 2, this study proposes that the strategic power island for that area encompass additional BAs within the state's boundaries as well as CAISO.[175] That would make the island still larger in terms of total load and generation within its footprint. Indeed, California is the fourth-largest total electricity producer in the nation.[176]

Yet, California also imports the second largest amount of electricity of any state after Virginia.[177] California utilities partly own and import power from several power plants in Arizona and Utah. California's electricity imports also include hydroelectric power from the Pacific Northwest, largely across high-voltage transmission lines running from Oregon to the Los Angeles area.[178] In recent years, California has been able to reduce its power imports by expanding generation inside the state, especially through utility-scale and DER solar installations.[179] Nevertheless, California continues to rely on electricity from outside the state.

None of these external power providers are included in the proposed power island for California. If that island were to segment from the grid and halt power imports, the state would face a sharp imbalance between load and generation. Emergency load shedding could restore that balance but at the cost of creating major disruptions for many customers. As an alternative, designers of the California island could expand its borders to include its external sources of power. But doing so would have ripple effects across other island configurations across much of the Western Interconnection, and would so greatly increase the size of the California island and the length of its transmission system lines that (as discussed above) the island might face increased risks of experiencing cascading failures.

Given the value of such flows for balancing operations on both sides of the border, US–Canada discussions on island design issues could be useful.

US–Canada Electricity Sharing

Power flows between the United States and Canada constitute an additional dependency for BAAs along the border and the power island that would be based on them. For decades, the United States has imported electricity from Canada and, to a much lesser extent, Mexico. The United States also exports power to Canada during periods when Canadian hydropower production declines. These electricity trades are relatively small, representing less than 1% of all US and Canadian generation. However, the EIA notes that this "is important to grid balancing—constantly matching electricity

[174] CAISO, "Balancing Authority."

[175] For a map of these additional California BAs, see California Energy Commission, "Balancing Authority Areas." For electric system topography reasons, it might make sense to include the two BAs in the far southwestern part of the state in the proposed Sun Country power island rather than its California counterpart. That level of detail is appropriate for the region's grid managers to address.

[176] EIA, "California Overview."

[177] EIA, "California Overview."

[178] On the power sources of energy imports, see EIA, "California Was the Largest Net Electricity Importer."

[179] California Energy Commission, "2024 Total System Electric Generation."

consumption to electricity production—and helping to shore up electricity supply during low hydropower production periods, particularly on the western coast of Canada."[180]

All such cross-border flows would terminate if US strategic power islands separated from the Western and Eastern interconnections. Given the value of such flows for balancing operations on both sides of the border, US–Canada discussions on island design issues could be useful. After all, Canadian BAAs are already part of the Western and Eastern interconnections (and are subject to the reliability and cyber protection standards of NERC). Follow-on studies might assess the potential benefits of adopting a binational approach to strategic power islanding.

Load Shedding in Generation-Poor Islands

For proposed islands that lack sufficient generation to serve all of the loads within them, separating from the grid and halting electricity imports will necessitate difficult decisions about which customers should lose power. RCs already employ emergency load shedding to maintain grid reliability when severe cold or other natural hazards disrupt power supplies. RCs also have the authorities and capabilities to do so in response to adversary-induced disruptions. Given this context, emergency load shedding in generation-poor power islands would have ample precedent.

However, the problems of such resource shortfalls are likely to intensify. A gap is emerging between supplies of electricity and demand for them in many US regions. NERC's *Long-Term Reliability Assessment* found that "the overall resource adequacy outlook for the North American BPS is worsening." Indeed, major portions of the United States, including the Pacific Northwest, ERCOT, and PJM's service territory, are at "high risk" for energy shortfalls.[181] A 2025 report by DOE warns that these risks to resource adequacy pose significant dangers for grid reliability. DOE found that with the retirement of thermal generators, their replacement by renewables with variable power output, and the growing power requirements for AI data centers and other loads, the "status quo is unsustainable" and (absent significant policy changes) threats to grid reliability will rapidly increase.[182] The Trump administration is advancing a range of initiatives to increase coal generation, nuclear plants, and other resources. For the near term, however, the challenges of balancing generation and load will be all the more difficult for strategic power islands.

To meet such challenges, island designers will first need to identify the available generation and load within each island under various contingencies (including peak load periods). In the absence of power exchanges between islands, *every* functioning generation resource will need to support emergency operations in resource-poor islands, even operations that typically are not employed because of their high costs.

The moment that interconnections shift from being a bulwark of resilience to a superhighway for spreading cascading blackouts, islanding makes sense.

Islands such as California will never have sufficient power to serve all of their loads. In those cases, industry and government leaders will need to specify which civilian and military loads are most critical and plan to serve only those facilities and

180 EIA, "U.S. Electricity Exports."

181 High-risk areas are those where "planned resources as of July 2025 would result in energy shortfalls that exceed resource adequacy targets or baseline criteria for unserved energy or loss of load." NERC, *Long-Term Reliability Assessment*, 6–7.

182 DOE, *Resource Adequacy Report*, 1.

functions for the duration of the emergency. Existing RC plans for manual load shedding provide a starting point for developing these plans and prioritizing the sustainment of power flows to water systems, hospitals, and major military bases. However, to enable fort-to-port operations and other complex military missions, few if any RCs or other grid entities will have mapped the web of mission-essential facilities and functions that will require electricity. The Department of War (DOW) should develop such maps and partner with DOE to share them in protected ways with island managers.[183]

Prioritizing service to critical civilian and military loads will create harsh (and, especially in the midst of severe weather, potentially deadly) conditions for families and other customers. However, in past severe weather events, utilities have conducted load shedding on an equivalent basis to prevent cascading failures. Operators typically begin that process by conducting manual load shedding designed to (1) "share the pain" by conducting rotating outages and (2) protect service to critical loads while cutting power to lower-priority customers. As in the case of California's August 2020 extreme heat event, such measures may be able to avert "uncontrolled load shed" and avoid "destabilizing the rest of the western grid."[184] If those measures prove inadequate, automatic load shedding can cut service to sequentially larger blocks of load as needed to get generation and load back into balance.

Emergency managers also have terrific expertise in preparing for life-threatening conditions in blackouts created by hurricanes or other natural disasters. DOE also informs these managers of the Defense Critical Assets in their service areas that could merit sustained service during manual load shedding or prioritized restoration if blackouts occur. However, it is not at all clear that TOPs, BAs, and DPs that help conduct load shedding will be aware of all of the facilities and infrastructure (military and civilian) necessary for power projection and other complex defense missions. DOW and DOE should continue their efforts to "disaggregate" their force deployment plans to identify customers that should be exempted from load shedding if at all possible, and securely share those data with the appropriate grid operators.

Island Separation in Grid Security Emergencies

The theory of when separation should occur is straightforward. The moment that interconnections shift from being a bulwark of resilience to a superhighway for spreading cascading blackouts, islanding makes sense. But determining that we have reached such a moment is enormously complicated and fraught with dangers.

Grid operators will have two basic options for segmentation. They can either separate islands based on grid conditions or do so in response to a determination by the president (in response to intelligence and warning, or I&W, indicators) that a potentially catastrophic attack is imminent or underway. Both options would be implemented by opening substation breakers for transmission tie lines that connect BAs, and power islands configured around them, with surrounding systems.[185]

These alternatives offer different mixes of risks and benefits against adversaries who will seek to manipulate, delay, and disrupt US decision-making. However, under both approaches, grid managers will not be making separation decisions in a policy vacuum. In any crisis that could lead to PRC attacks on the grid, government leaders will have powerful incentives to help industry defend their systems. They also have extraordinary authorities to do so.

183 For detailed recommendations on developing and sharing data on mission-critical infrastructure and functions, see DOD DSB, *Department of Defense Dependencies*, 6, 9.

184 CAISO conducted rotating outages as part of its manual load shedding. CAISO, *Root Cause Analysis*, 30–31.

185 NERC, *Balancing and Frequency Control*, 2.

Under the Federal Power Act (FPA), the president can declare a grid security emergency (GSE) when they determine that attacks are underway or are in "imminent danger" of occurring. Once the president declares a GSE, the secretary has the authority to order BPS entities to do *whatever* the secretary deems necessary to "protect or restore" critical electric infrastructure.[186]

DOE has conducted planning and exercises with industry on how GSE orders might direct utilities to prioritize the restoration of power to critical defense facilities and other essential loads. However, no equivalent progress has been made on GSE orders to protect the grid when attacks are imminent or underway. Grid owners and operators will not wait for such orders before taking emergency actions to defend their systems, including measures to prevent or halt the spread of cascading outages. But in an intensifying crisis with China, the energy secretary may also issue GSE protection orders that advance specific national security priorities. It will be better for industry and government to discuss possible orders in peacetime rather than develop them from scratch during a grid emergency. Orders to segment strategic power islands when a PRC attack is imminent offer a potential focus of such discussions.

Islanding on warning carries downside risks. Given the disruptive effects that separating from the grid would have on electric service, especially for islands that lack sufficient generation resources to serve all the loads within them, Chinese leaders might be tempted to "spoof" the system and provoke islanding even if they do not plan to actually attack—though any such action would risk incurring US responses and a rapid escalation of conflict.

186 Under the FPA, the president can declare a GSE in response to physical attacks, cyberattacks, electromagnetic pulse attacks, or a geomagnetic storm events that have significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as defined by the act (16 U.S.C. § 824o–1). This report's analysis of GSEs also relies on DOE, "Grid Security Emergency Orders."

A greater risk may be that because islanding would be so disruptive, the president might hesitate to issue GSE orders for separation until attacks were underway and already creating massive grid disruptions. And, most dangerous at all, failures of US I&W systems could enable China to conduct a surprise attack and preempt our efforts to island.

Standing up islands on condition would avoid these pitfalls. Conditions-based separation would also maximize opportunities for emergency actions to mitigate instabilities, prevent cascades from beginning, and preclude the need for islanding. To reiterate a key point of this study: keeping interconnections up and running if at all possible will *always* be preferable to islanding. However, if the PRC can overcome our emergency actions and cascades begin, the speed with which they will propagate out could delay conditions-based islanding until outages have covered much or all of the United States. China will also do everything it can to disrupt or manipulate the sensors and other systems that assess grid conditions.

Every separation strategy carries risks. The question is, which approach offers the best opportunities for risk mitigation against a sophisticated, adaptive adversary?

Separation on Condition

As noted in the Current Fallback Defenses section, RCs and other BPS entities have sophisticated sensors and capabilities to maintain the stability of the interconnections and limit the impact of natural or adversary-induced disturbances. Many of these same capabilities can not only help operators prevent cascading outages from occurring but also facilitate islanding on condition if prevention measures begin to fail. The same is true of the specific metrics and assessment tools that operators employ when severe grid disturbances occur.

A (Very) Rough Cut on How Separation Could Occur

The preplanned use of protection systems or other control systems to separate part of the BPS into intentional islands lies at the core of conditions-based strategies. These points of separation are specifically designed to operate based on local detection or remote transfer trip signals. As part of that design effort, NERC notes that the "separated systems have been studied to perform acceptably for the specified contingency events."[187] But additional technical analysis and preplanning will be required to implement such an approach. In particular, system protection engineers will need to analyze whether and how those systems could automatically segment islands in the face of extreme adversary-induced instabilities. The basic concept is clear-cut. Relays, circuit breakers, and other protection system components would be set to conduct separation upon specified grid conditions within the milliseconds needed for protection against cascading failures. The details that underlie this concept are more problematic.

Protection systems are not designed to enable preplanned islanding, and it is not clear how they could perform that function in a reliable, low-risk way.

One challenge is specifying the conditions that should trigger separation—not too early, but also not too late. Data gathered pursuant to NERC *IRO-009-2—Reliability Coordinator Actions to Operate Within IROLs* can help operators make these determinations. IRO-009-2 is intended to help operators "prevent instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the interconnection by ensuring prompt action to prevent or mitigate instances of exceeding Interconnection Reliability Operating Limits (IROLs)."[188] An IROL is "a System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System."[189] NERC's *Methods for Establishing IROLs* provides detailed recommendations for cascading analysis assessment techniques (including probabilistic and risk-informed methodologies), overload thresholds, tripping factors, and other guidelines that might be useful to support the development of conditions-based separation criteria.[190]

However, protection systems are not designed to enable preplanned islanding, and it is not clear how they could perform that function in a reliable, low-risk way. One option might be to set underfrequency relays on the electrical boundaries of islands to open when frequency drops reach a certain level, just as they open to protect generators and other equipment in typical underfrequency events.[191] This approach would entail a host of problems. Steve Naumann, former vice president for transmission and NERC policy at Exelon, cautions that frequencies might not drop low enough to actuate the relays before cascades begin. Another TOP interviewed for this study stated that the telemetry needed to arm underfrequency relays and enable other automated islanding functions may not be adequate for these purposes, versus for normal relay operations.

As an alternative, BAs could set "islanding relays" on BAA boundaries to trip based on specified power and under- and overvoltage swings. However, even

[187] NERC, *Reliability Guideline*, 67–68.

[188] NERC, *IRO-009-2*.

[189] NERC, *Glossary of Terms*, 23. In turn, system operating limits are "Facility Ratings, System Voltage Limits, and stability limits, applicable to specified System configurations, used in Bulk Electric System operations for monitoring and assessing pre- and post Contingency operating states." NERC, *Glossary of Terms*, 42.

[190] NERC, *Reliability Guideline*, 74–89.

[191] NERC, *PRC-006-2*.

with the increasing sophistication of microprocessor relays and sensors, it will be immensely difficult to set relays to differentiate between severe but recoverable swings versus nonrecoverable, potential cascading swings. Put another way: we would need to ensure that relays open when cascades are imminent and *not* open in the face of other, less severe disturbances that BAs can manage with emergency actions. In fact, if such unnecessary islanding occurred, the disruptive voltage and frequency impacts on surrounding electric systems would exacerbate the attack's effects.

Research should go forward to examine these problems and potential solutions, including improved use of sensor data and AI-enabled analytics to deal with the incredibly short decision space available for islanding on condition. One possible area of focus: explore whether and how operators (and their decision-support tools) might use wide-area PMU data to supplement data on voltage, frequency, and power swings to determine when cascades are imminent and islanding should occur.

A further challenge lies in coordinating separation across neighboring BAAs. As with implementing RAS, segmenting an island and halting cross-BAA power exchanges could inflict significant disturbances on surrounding systems.[192] The best way to mitigate those effects would be for all of the islands in a region to coordinate the split-second timing of their separation. However, NERC has found that RCs "vary widely" in the criteria and methodologies they use to assess whether "cascading events are acceptable" because they are likely to cease or whether they are "unbounded" and will progress to an unknown operating state.[193] These variations will complicate efforts of neighboring RCs and BAs to coordinate conditions-based islanding and avoid fratricide across their systems.

Adversary Manipulation of Conditions-Based Islanding

If the United States adopts islanding on condition, adversaries will almost certainly seek to exploit the vulnerabilities of segmentation-related hardware, software, and operations. The 2003 blackout is instructive in this regard. The US–Canada report on that event found that failures in alarm systems, emergency management systems, primary and backup servers that supported warning functions, and other systems hobbled the ability of FirstEnergy (a TOP in Ohio) to halt the spread of instabilities that originated in its service territory. The result: "For over an hour no one in FE's [FirstEnergy's] control room grasped that their computer systems were not operating properly," and "without a functioning EMS or the knowledge that it had failed, FE's system operators remained unaware that their electrical system condition was beginning to degrade" and that emergency actions were urgently needed.[194]

EMS and alarm systems are vastly more sophisticated today than in 2003. However, FirstEnergy's systems failed even without enemy efforts to disrupt them. Future adversaries are likely to conduct Volt Typhoon-style LotL attacks or other measures to misoperate these systems, display false data to operators, or otherwise deny or corrupt the situational awareness on which emergency actions depend.[195] These same attack vectors could delay conditions-based islanding until cascades were underway.

The automatic functioning of relays and circuit breakers at specified conditions and other settings could provide a fallback against such operator-level failures if the technical problems and operational risks of employing such island relays could be overcome. However, these digital devices and

[192] NERC, *PRC-012-2* requires RCs and planning coordinators to assess and mitigate these potential impacts.

[193] NERC, *ERO Enterprise*, 20.

[194] US-Canada Power System Outage Task Force, *Final Report*, 51–54.

[195] CISA, "PRC State-Sponsored Actors."

their software offer lucrative targets for disruption or misoperation as well. Preparedness for such exploits is limited. Operators have zero real-world experience with assessing and mitigating simultaneous attacks on multiple grid-control sensors and protection systems. Moreover, as in the final stages of the 2003 blackout, cascading failures can spread across multistate regions in seconds.[196] For all these reasons, relying on conditions-based segmentation would entail enormous risks.

Separating on I&W

Even if BAs and other BPS entities prefer a conditions-based strategy and the opportunities that strategy creates for taking emergency actions to sustain the interconnections and (ideally) avoid the need for islanding, they may not have the opportunity to follow that approach. A large-scale attack on the US grid would almost certainly occur in the context of an intensifying international crisis in the Taiwan Strait or some other regional flash point. If such a crisis were to intensify and the risk of war to increase, the president might well declare a GSE and direct the secretary of energy to begin issuing GSE orders—including, potentially, to separate strategic power islands from their interconnections.

Warning-based separation would be less vulnerable to enemy manipulation of the digital systems and data flows essential for separating on condition.

The FPA defines GSEs as the occurrence or imminent danger of cyberattacks, physical attacks, and other specified threats that could have "significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure" as the result of such attacks. In turn, "critical electric infrastructure" means a system or asset of the BPS, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters.[197]

Every large BAA (and many small ones) operates critical electric infrastructure. As a result, they could be subject to GSE orders in future crises. Some of these BAAs also include defense-critical electric infrastructure, defined as "any electric infrastructure located in any of the 48 contiguous States or the District of Columbia" that serves a critical defense facility.[198] However, only a limited number of BAAs have critical defense facilities in their service areas. The islands configured around those BAAs, and the critical facilities within them, will offer prime opportunities for the development and exercise of template orders that would be modified as necessary when attacks occur.

The secretary of energy has wide latitude in shaping these orders once the president declares a GSE.

> Whenever the President issues and provides to the Secretary a written directive or determination identifying a grid security emergency, the Secretary may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric

[196] US-Canada Power System Outage Task Force, *Final Report*.

[197] 16 U.S.C. § 824o–1, (a)(7). The president and secretary of energy also have other authorities, including Section 202(c) of the FPA, they might employ in grid emergencies. But that section focuses on ordering "temporary connections" of grid infrastructure rather than separation into islands. DOE, "DOE's Use of Federal Power Act."

[198] 16 U.S.C. § 824o–1, (a)(4). Critical defense facilities are "facilities located in the 48 contiguous States and the District of Columbia that are— (1) critical to the defense of the United States; and (2) vulnerable to a disruption of the supply of electric energy provided to such facility by an external provider." 16 U.S.C. § 824o–1, (c).

> infrastructure or of defense critical electric infrastructure during such emergency.[199]

Issuing orders to segment strategic power islands from the grid would fall well within this grant of authority. And if grid managers, regulators, and government leaders did indeed develop islanding as an emergency option, having it in the president's GSE toolbox could offer novel benefits as well as risks.

The Upside of GSE Orders to Island

BAs could island on warning during a crisis based on their own assessment that war looms. The electric industry is discussing ways to structure an international threat assessment framework to help utilities decide when to begin emergency operations when risks of attacks are increasing, just as they rely on weather predictions to assess hurricane storm tracks to shape their preparedness efforts. The advantage of separating on warning is that segmentation would be certain to occur. Especially important, warning-based separation would be less vulnerable to enemy manipulation of the digital systems and data flows essential for separating on condition.

If industry and government adopt an on-warning strategy, both would benefit from relying on GSE declarations rather than industry-generated threat assessments. Utilities will never have access to the real-time threat data that the US intelligence community (IC) provides to the president and that could help determine that attacks on the grid are imminent. Intelligence warnings are far from foolproof. As will be discussed below, enemies may attempt to "spoof" the president and secretary into ordering island separation (and the disruptions that would create) when they have no immediate plans to attack. But such provocative actions would be extraordinarily dangerous to the perpetrator given the additional ways in which the United States might respond.

Using GSE orders to initiate islanding would have additional benefits beyond greater certainty of warning. The first is communications with the public. The Electricity Subsector Coordinating Council (ESCC) and its members have extensive "playbooks" for messaging customers during outages caused by severe storms or other natural hazards. But no utility CEO will want to get out in front of the president in messaging during an international crisis, much less on why power islanding is necessary.[200] The presidential declaration of a GSE and accompanying leadership messages to the public will provide crucial "top cover" for potentially drastic emergency actions by grid operators.

Industry and government could also jointly develop a set of incremental orders to facilitate a phased approach to islanding. If the IC were to determine that the likelihood of a PRC attack was growing, GSE orders could direct island operators to take sequential measures prior to actual separation, starting with "normal" actions that TOPs already use for conservative operations and emergencies and then moving to islanding-specific measures as threats intensify.

Normal actions:

- Require managers and GOs to bring additional generators online, including coal-fired resources that will take more than twelve hours to start up, and prepare to go to maximum generation.[201]
- Suspend wholesale energy markets that drive utilities in organized markets to purchase low-cost resources (often from neighboring BAAs) and establish a fixed price for all energy purchases regardless of price.
- Order asset owners to return transmission lines and generators from maintenance.

[199] 16 U.S.C. § 824o–1, (b)(1).

[200] ESCC, ESCC Brochure.

[201] EIA, "About 25% of US Power Plants."

Actions to take if the president determines that the risks of attack are growing:

- Prepare to operate in the absence of EMS or SCADA systems (or to do so if adversaries corrupt these systems).[202]
- Confirm which specific tie lines will be opened and ensure that operators are prepared to implement separation orders.
- Confirm load-shed plans for prioritized manual load shedding and, if necessary, automatic shedding of large blocks of load.
- Just before separation, initiate gradual load shedding and reduce power imports in generation-poor islands to limit the danger that when separation occurs, surrounding areas will experience high-voltage and high-frequency events that could cause generation trips and other instabilities.

Once these and other preparatory measures are in place, island managers could coordinate with government leaders on exactly when separation will take place, with those managers adjusting their systems as needed until they open the final breakers and begin independent operations.[203]

The FPA has established a process under which such coordination and collaborative planning could go forward. The act states that before issuing GSE orders, the secretary of energy shall, "to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action," consult BPS entities, the ESCC, and a range of government authorities.[204] DOE and potential GSE order recipients should exercise the use of such consultative mechanisms and ensure that survivable communication systems can support them.

202 NATF, *Bulk Electric Systems Operations.*

203 My thanks to Steve Naumann for making these recommendations.

204 16 U.S.C. § 824o–1, (b)(3).

Problems with Relying on GSE Orders

While adversaries may accept the escalatory risks of spoofing the secretary into ordering separation when they do not intend to attack and thereby disrupting electric service to the public and (perhaps) corroding the government's credibility, other problems could be more likely to occur. A former BPS regulator warns that "putting the trigger for islanding in the hands of the president alone seems rather risky. We could have an X post and the entire grid would segment, disrupting reliability on a whim." The actual process of determining that a PRC attack is imminent would presumably be much more structured and reflect significant input from the IC. Nevertheless, the former regulator made an important point: "ISO, RTOs, and utilities have the most detailed and accurate understanding of grid reliability and resilience, and relying on GSE orders would pull authority away from them."

Adversaries may disrupt the communications channels DOE uses to transmit GSE orders to island or use deepfakes to corrupt such messaging.

The best way to mitigate the risks of poorly informed GSE orders is for DOE to closely collaborate with industry on the design, timing, communication, and implementation of potential orders. DOE should continue to strengthen industry–government planning accordingly.

Prerequisites for Effective Separation on Warning and the Benefits of a Hybrid Strategy for Separation

The worst possible time to begin consultations on GSE orders is in the midst of an attack. DOE and the ESCC began discussing emergency orders shortly after Congress enacted these FPA emergency amendments in December 2015. However, they have made only limited progress in developing "template" GSE orders for likely recipients that could be adjusted during emergency consultations to address attack-specific circumstances. The industry–DOE discussions that have occurred have focused exclusively on power restoration rather than measures to protect the grid before attacks occur. As grid operators assess future options for islanding and other extraordinary protective measures, DOE should be a partner from the start in aligning these options with broader federal planning for grid security emergencies.

It would be prudent for grid operators to have fallback, conditions-based capabilities to create islands once attacks are underway.

Islanding on warning of a GSE carries risks as well. Although unlikely, it is conceivable that an adversary might launch a "bolt from the blue" attack and strike the grid in the absence of an escalating crisis or any other identifiable threat indicators. A more serious risk is that adversaries may disrupt the communications channels DOE uses to transmit GSE orders to island or use deepfakes to corrupt such messaging. DOE initiatives to secure such communications links will need to scale with the intensifying nature of those threats. As a backstop against such disruptions, it would be prudent for grid operators to have fallback, conditions-based capabilities to create islands once attacks are underway.

An additional advantage of adopting such a hybrid approach lies in its potential value for deterrence. If the United States can stand up power islands as a crisis intensifies and reduce adversary leaders' confidence that cascading failures will cut off power to America's critical defense and nondefense facilities, those leaders may be less likely to strike the grid. Issuing GSE orders to island, combined with explicit messaging to Xi Jinping or other potential adversaries, including on the potential costs they might incur by attacking, could help strengthen deterrence.

Achieving such benefits will depend on convincing enemy leaders that strategic power islands can not only wall off cascading outages but also survive targeted attacks on the infrastructure within their boundaries. Otherwise, these islands will be useless for deterrence and for sustaining service to critical loads if deterrence fails.

A hybrid strategy entails an additional problem—one that cuts to the heart of the dilemmas of islanding. If grid managers and their government partners separate on I&W (with conditions-based separation occurring only as a fallback), operators will foreshorten their ability to use emergency actions to stanch instabilities and keep the interconnections up and running. In events that turn out in retrospect to have been recoverable, islanding will nevertheless occur if threats of attack cross a predefined threshold. The downside of I&W-based separation is we could break up the interconnections when doing so is unnecessary and cascades are still preventable. The compelling upside: separation will occur in ways that are far more certain (and less vulnerable to adversary manipulation) compared with conditions-based strategies.

Integrating Power Islands and Restoring the Interconnections

Successful islanding (and the sustained service of critical loads) should ultimately support a broader goal: the reestablishment of the interconnections and the reliability benefits that they offer. When RCs, TOPs, and their partners determine that adjacent islands are sufficiently stable, operators must synchronize the islands by matching voltages, phase angles, and frequencies at the connection points to consolidate them.[205]

[205] Garcia et al., *Hydropower Plants,* 2.12. RTOs/ISOs overseeing blackstart operations might have "designated synchronization points" for connecting islands. See ERCOT, *ERCOT Nodal Operating Guides*, 4–18.

Island integration will be technically complex because each individual island will likely be out of synchronization with surrounding islands. To connect two islands, operators will need to coordinate their respective frequencies to achieve synchronization.[206] Failure to do so before connecting their islands could damage equipment and cause generators to trip off, potentially leading to island collapse. Once islands are reconnected and power flows between them are restored, additional procedures and control mechanisms will be needed to manage such exchanges.

Once an RC has integrated all the islands within its own reliability control area, it must synchronize it with neighboring RCs to reconstitute the grid. Depending on resource availability and other factors, an RC may also decide to connect to neighboring RCs before all islands in the RC control area are consolidated. In either case, NERC standards require RC restoration plans to include criteria, conditions, and training programs for reestablishing interconnections with other RCs.[207] Even with detailed planning and exercises, however, the process of reintegration will be difficult and complex—all the more so if adversary attacks on the grid continue.[208] Sustained progress to meet these challenges must be an integral component of strategic islanding regardless of which option the United States ultimately adopts for separation.

Island Vulnerabilities and Mitigation Measures

Initial drafts of this study were based on a mistaken premise. Drawing on *Surfing the Wave*, the study began by proposing that strategic power islands should leverage the ongoing transformation of the US generation fleet that has been driven by (1) the deployment of millions of solar DERs and larger BPS-connected solar plants and (2) the nationwide installation of BESS to manage the intermittency of solar generation and, increasingly, provide ancillary services to help maintain the grid's reliability.[209] The study's initial hypothesis: the spread of these new energy resources across the United States enabled the creation of strategic power islands to an extent that was never before possible.

An alternative approach turns out to make better sense. If the United States makes islands big enough, they are *certain* to have large numbers of conventional, large-scale generation resources within their perimeters, as well as solar and BESS installations. As of December 2022 (which is the latest update provided by the US Energy Information Agency), there were 25,378 electric generators at about 12,538 utility-scale electric power plants in the United States—that is, plants that have a total electricity generation capacity of at least one megawatt.[210] Since then, the deployment and expansion of new generators has greatly increased their number and widespread distribution, with 468,582 megawatts of new generation currently under development across the United States.[211]

Every strategic power island proposed in the Current Fallback Defenses section will encompass hundreds of such assets. The expansion of in-island

[206] This is conceptually similar to synchronizing a generator to the system on startup but will be more difficult because of the islands' lower system inertia.

[207] NERC, *EOP-006-3*, R1.2, R7.

[208] For a detailed assessment of these challenges, see NERC, *EOP-005-3*, R1.9; NERC, *EOP-006-3*, R1.6; and Stockton et al., *Electric Infrastructure Protection (EPRO) Handbook V*.

[209] Developers added twelve gigawatts of new utility-scale solar electric generating capacity in the United States during the first half of 2025, and they plan to add another twenty-one gigawatts in the second half of the year. That would make solar account for more than half of the sixty-four gigawatts that developers plan to bring online this year. Battery storage, wind, and natural gas power plants account for virtually all of the remaining capacity additions for 2025. Smaller DER deployments add still further to this growth, though Trump administration policies are likely to slow that expansion. EIA, "U.S. Developers."

[210] EIA, "How Many Power Plants."

[211] Buttel, *America's Electricity Generation.*

generation will grow as industry and the Trump administration press to deploy additional thermal, advanced nuclear, and enhanced geothermal resources.

Relying on BPS resources instead of DERs alone has compelling advantages. As discussed in the section PRC-Induced Cascading Failures, natural gas turbine generators can be rapidly dispatched to meet spikes in demand and help island managers balance generation with load. The turbines and other spinning masses in gas, coal, nuclear, and hydro plants also provide system inertia that could help keep islands stable in the face of adversary-induced disturbances. BESS and other DERs using advanced inverter technologies are gaining the ability to provide some of these features as well. In the meantime, however, BPS thermal, hydro, and nuclear resources will be superior contributors to island resilience.

Security factors magnify this advantage. BPS generators are subject to mandatory, enforceable cyber and physical security standards established by FERC and NERC. DERs are regulated by states and have no remotely equivalent set of enforced security mandates. Moreover, FERC and NERC continuously update and expand their security standards to keep pace with increasing threats (though the lack of requirements to counter UASs remains a critical gap). A growing number of states are strengthening DER cybersecurity standards as well. That progress is slow, however, with wide variations in the adequacy of state mandates versus voluntary cybersecurity guidelines.[212] Structuring islands to rely primarily on BPS assets and operations, including generation, transmission, and control centers, offers enormous advantages.

Aggressive measures will be required to stay ahead of PRC attack capabilities against the US interconnections and power islands designed to separate from them. NERC's 2025 assessment that "industry cannot keep pace with resilience threats" applies not only to the BPS, but also to the BPS components on which islands would depend. Most important, utilities and their government partners must mitigate the danger that equipment, firmware, and software deployed in islands nationwide will be vulnerable to common mode failures and that attacks exploiting those vulnerabilities will be able to create the functional equivalent of cascading blackouts.

Countering Adversary Disruptions

In addition to adopting the mitigation measures proposed by *Surfing the Wave* against supply chain exploits, LotL attacks, and the massive, rapid manipulation of electrical loads, island managers will need to tackle difficult coordination and incident response challenges. Structuring islands to depend on BPS resources as well as DERs begs the question: how will managers control the significant and growing DERs within their borders and effectively use them for balancing, frequency control, and other functions essential for island reliability in the face of adversary attacks?

Collaboration between two different types of entities will be crucial for emergency operations. The first is BAs. Beyond their intimate familiarity with the electric infrastructure in their BAAs and the expertise they have derived from balancing load and generation during incidents, there are additional persuasive reasons to make BAs responsible for island management. BAs also have the authority to direct utilities that are DPs to shed load during emergencies to help manage frequency disturbances. In addition, every BA has tailored incident response protocols and can declare energy emergency alerts to take additional actions, including measures to sustain service to hospitals, water utilities, and other critical customers if rotating power outages occur within a BAA.[213] All of these measures—in addition to the support that BAs will

[212] Stockton, *Surfing the Wave*, 7–9, Appendix C.

[213] DOE, "How It Works," 1, 3–6.

receive from RCs, TOPs, and other BPS entities—will be useful against cyberattacks on segmented islands when disruptions occur.[214]

DPs will play a crucial role in island defense as well given the significant penetration of DERs in most BAAs and the islands on which they would be based. DOE defines DPs as "any utility that owns, operates, or controls facilities used for the distribution of electric energy."[215] The FPA explicitly excludes such distribution systems from its definition of the BPS, and these systems are not subject to NERC's reliability or security standards.

Yet, because of rapid DER growth and the increased flow of power from these resources to the BPS, BAs must be able to coordinate with DPs to perform balancing and other reliability functions.[216] The benefits of coordination will be all the greater as states require that DER inverters be able to ride through disturbances (versus immediately shutting down) and also provide voltage and frequency control capabilities recommended by IEEE Standard 1547.[217] Strategic power island resilience planning should take advantage of these capabilities to help ensure that DERs can assist with implementing island defense planning and operations by BAs.

Island defense coordination between BA and DER operators will be complicated by the diversity of these operators. In theory, DPs might serve as a single point of contact for them vis-à-vis BA control rooms. In practice, DER operators include energy aggregators, virtual power plants, and other entities that typically have little or no cyber expertise, much less experience in supporting BA-wide defensive operations.

FERC Order 2222, *Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators*, provides a basis for progress. In addition to facilitating the inclusion of DER-provided power in wholesale energy markets, the order directs grid operators to establish operational coordination mechanisms to manage the interactions between transmission and distribution systems in real-time operations. It requires establishing a process for ongoing coordination that addresses communications among RTO/ISOs, aggregators, and the distribution utilities. The order also requires aggregators to report to their RTO/ISOs any changes to the power they offer due to DER asset outages/curtailments. Furthermore, the order requires coordination protocols and processes for the operating day that allow distribution utilities to override RTO/ISO dispatch of a DER aggregation under circumstances "where such override is needed to maintain the reliable and safe operation of the distribution system." This includes the protocols for communications, control, and response when there are changes in DER output or system conditions.[218] All of these provisions will be useful for coordinated BA/DER cyber defense in power islands.

---

[214] Note that in islands built around the BAAs managed by RTOs and ISOs, those organizations serve as both BAs and RCs. RCs have the highest authority to prevent or mitigate grid emergencies by managing grid conditions, generation, and demand and protect BPS reliability in the face of cyberattacks or other hazards. For strategic power islands in non-RTO/ISO service areas, other coordination mechanisms exist between RCs and BA island managers.

[215] DOE, *Distribution Standard of Conduct*, 3. NERC offers a different and more detailed definition. A DP "provides and operates the 'wires' between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner is also the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the distribution function at any voltage." NERC, *Glossary of Terms*, 14.

[216] Denholm and Cochran, *Balancing Area Coordination.*

[217] For a discussion of the benefits of these inverter capabilities for cyber incident management and a strong endorsement by state regulators that states the guidelines in IEEE 1547, see NARUC, *Cybersecurity Baselines.*

[218] FERC, *Final Rule*. See also DOE, *TSO-DSO-Aggregator Market*.

TOP and BA personnel interviewed for this study reported that BA–DP collaboration is rapidly improving. BAs and the distribution providers in their areas are sharing increasingly detailed data on the electrical equipment in their footprints. This includes the information on transmission-to-distribution interfaces (T-D Interface), distribution system layouts, aggregate load, and DER deployments. A 2023 NERC report written in collaboration with DPs emphasized that the study participants "did not identify a need for a broader collaboration of data sharing improvements to operations horizon outside of ensuring the T-D Interface is monitored for their appropriate flow conditions and representations of the load and generation at the T-D Interface."[219] However, this finding should be reviewed in light of the coordination problems that emerged with distribution system operators during the Iberian blackout, including loss of communications "and insufficient observability of facilities involved in bottom-up restoration scenarios of distribution grids."[220]

While this data sharing provides a foundation for coordinated defense, especially by enabling shared situational awareness by DPs and BAs, progress has only begun to create joint cyber incident response plans that include DER and BPS assets and operations under the BA's control. If the electricity subsector and its government partners go forward with strategic power islanding, the development and exercising of such plans should be a top priority.

Natural Gas Fuel Deliveries as an Additional Problem for Island Resilience

Natural gas-fired generators offer immense benefits for real-time dispatch, frequency control, and other island reliability functions. However, relying on such generators also entails a risk: adversaries may seek to disrupt the pipelines that fuel them. DOW assesses that China can launch cyberattacks attacks that could cause the "disruption of a continental United States natural gas pipeline" for "days to weeks" together with other infrastructure damage.[221]

If the PRC attacks the US electric system, it is sure to strike gas infrastructure as well. Island planners will need integrated gas–electric resilience strategies to ensure that adequate generation will exist to serve critical loads.

The potential impact of such attacks on strategic power islands will vary by US region. Figure 4 depicts US natural gas pipeline infrastructure.

Some US regions and the proposed power islands associated with them, including the southern portion of the MISO service area and the Marcellus shale region in the northern part of PJM, have highly redundant pipeline infrastructure as well as nearby gas production and processing facilities. That redundancy provides a bulwark of resilience against adversary attacks.

New England is at the opposite end of the resilience spectrum. The BA for the region, ISO New England, and the proposed island on which it would be based rely on natural gas-fired generators for 50% of New England's power. The limited network of natural gas pipelines serving those generators already threatens grid reliability in the region.[222] If the PRC attacks the US electric system, it is sure to strike gas infrastructure as well. Island planners will need integrated gas–electric resilience strategies to ensure that adequate generation will exist to serve critical loads. They will also need load-shedding

219 NERC, *Transmission and Distribution*, 2–3.

220 ICS Investigation Expert Panel, *Final Report*, 26.

221 DOW, *2025 Annual Report*, 18.

222 Levitan and Associates, *Northeast Gas/Electric System Study*.

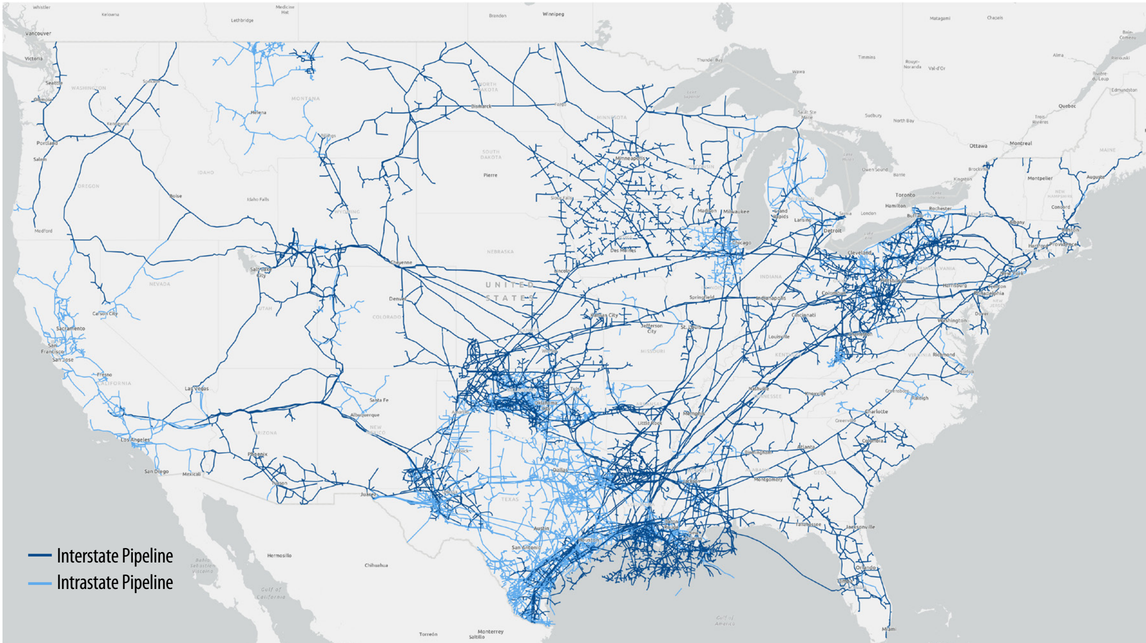

Figure 4. US Natural Gas Pipelines

plans to employ *in extremis*. The same is true for California and other proposed islands that heavily rely on gas generation but are served by a limited number of interstate pipelines.

NERC's 2025 *Long-Term Reliability Assessment* cites the risk of gas system interruptions as a significant challenge facing the BPS.[223] Interruptions could also jeopardize the operation of strategic power islands in many US regions. If industry and government leaders move forward on islanding, nationwide and region-specific progress on natural gas system resilience (especially the build-out of additional pipeline infrastructure) will be essential.

Deterrence

As summarized by the DSB *Task Force on Cyber Deterrence*, "deterrence operates by affecting the calculations of an adversary, specifically by convincing the adversary that the expected costs of a potential act (a type of attack or costly cyber intrusion) outweigh the expected benefits."[224] Strategic power islands can influence both factors in such adversary assessments. Islands may be able to bolster the ability of US strike forces and their installations to respond to adversary attack and thereby strengthen deterrence by cost imposition. But microgrids already serve the same purpose in many such bases. The more compelling benefits of strategic power islanding lie in deterrence by denial—that is, in reducing the benefits that PRC leaders expect to gain by attacking the grid, including by disrupting the flow of US forces to East Asia in future crises and inciting societal panic.

Deterrence by Cost Imposition

The DSB Cyber Deterrence study emphasizes that "reducing the vulnerability of U.S. critical infrastructure is essential not only to deterrence by denial, it also reinforces the credibility of U.S. threats to impose costs on attackers." In particular, "due to the centrality of electrical power generation in supporting military strike capabilities, the cyber

223 NERC, *Long-Term Reliability Assessment*, 11, 178.

224 DOD DSB, *Defense Science Board Task Force*, 3.

security and resilience of electrical power deserves particular attention."[225]

Since the publication of the DSB study in 2017, DOW has constructed hundreds of additional emergency power resources and microgrids to strengthen the power resilience installations that perform strike-related missions. At Naval Submarine Base Kings Bay, which supports the Trident Submarine Ballistic Missile fleet, the Navy is constructing a forty-two-megawatt solar installation and BESS facility to power the base and its critical functions in the event adversaries black out the grid.[226] Microgrids are also being proposed for strike-related installations such as Offutt Air Force Base, headquarters of the US Strategic Command, to cover "immediate critical mission gaps."[227]

For bases that are critical to deterrence by cost imposition, the United States should consider adopting a "belt and suspenders" strategy.

The PRC-Induced Cascading Failures section noted that relying on emergency power systems and microgrids can entail risks to DOW mission execution. For example, military bases typically rely on electricity-dependent water systems infrastructure beyond their fence lines and will lose those support systems in wide-area blackouts. But the extent of these vulnerabilities (and the adequacy of emergency power and microgrids for energy resilience) will vary with the types of missions that an installation performs. For large-scale bases that perform sustained operations and maintenance activities, such as Naval Station Norfolk, and those responsible for readiness, training, and deployment-related functions for thousands of troops, such as Fort Hood, dependence on outside-the-fence-line public infrastructure is extensive.[228] Expanding defense microgrids to encompass all of these support functions would be costly and technically challenging.

In contrast, installations responsible for launching cyber, nuclear, or conventional strike forces have been weaning themselves from external dependencies for years and are excellent candidates for the deployment of additional emergency power capabilities and microgrids scaled for extended conflicts.

It would be nonsensical to abandon efforts to strengthen such backup power initiatives in favor of strategic power islanding. Rather, for bases that are critical to deterrence by cost imposition, the United States should consider adopting a "belt and suspenders" strategy. If grid managers and government leaders can overcome the many impediments to making strategic power islanding viable, islands could provide a layer of defense against cascading blackouts when BA and RC emergency actions prove inadequate. Then, within these islands, strike-related bases would rely on their own microgrids as a hedge against island disruptions. This combined approach could help undermine any hope enemy leaders have of escaping punishment if they cause interconnection-wide outages.

Deterrence by Denial

The DSB study found that the United States will need to tailor cost-imposition strategies to individual countries and hold at risk the targets that specific adversary decision-makers value. The report also recommended that the United States be able to communicate (explicitly and/or implicitly by

[225] DOD DSB, *Defense Science Board Task Force*, 17–18.

[226] USN, "Groundbreaking Ceremony."

[227] OUSW(C), *FY 2024 Energy Resilience*, 175.

[228] Installations that comprise the Naval Station Norfolk depend heavily on water provided by Norfolk's municipal water system and other public infrastructure. City of Norfolk, "City of Norfolk Utilities." Fort Hood relies on water services provided by the Bell County Water Control District and the American Water company's distribution system. American Water, *2022 Annual Water Quality Report*.

presidential action) the credible will and capability to respond to cyberattacks on US infrastructure and other targets.[229] Equally valuable, if less widely recognized: the United States should adopt a tailored approach to strengthening deterrence by denial against the PRC.

The starting point to do so lies in the US IC's assessment of China's objectives in attacking US infrastructure in future crises. Such attacks would be designed to deter US military action by (1) impeding US decision-making; (2) inducing societal panic; and (3) interfering with the deployment of US forces.[230]

Previous sections of this report have already examined the potential advantages of islanding over microgrids to counter the first two of these goals. Public health and safety depend on millions of community health care facilities, grocery stores, water and wastewater systems, and other electricity-dependent assets and functions. PRC leaders may hope that disrupting the flow of power to these customers will help induce social panic. And if panic and looming health crises result from grid attacks, US decision-makers would face mounting pressures to back down in a confrontation with China. In particular, they may decide that the benefits of defending Taiwan or other US regional allies are not worth the costs of doing so and thereby help China achieve its overarching goal of deterring US military action. The ability of power islands to sustain service to critical public health and safety facilities would help the United States counter all such objectives.

Yet, these capabilities alone are not sufficient to strengthen deterrence by denial. The United States must also persuade Chinese leaders who are weighing the potential costs and benefits of an attack that islanding will be successful. Realistic exercises would bolster such efforts but would also present unprecedented challenges for power companies and government leaders. Grid managers frequently use tabletop exercises and training to strengthen preparedness for extreme events. None of these exercises, however, involve actual grid disruptions. For example, TOPs *never* practice blackstart restoration under "real world" conditions, which would require blacking out major portions of their service areas. For the same reason, BAs will be extraordinarily reluctant to practice islanding and all the service disruptions that separating from the grid would entail.

The exercising of sequenced GSE orders might help shape adversary perceptions while also staying within the comfort zone of grid operators. Well-publicized exercises could begin with the simulated issuance of orders to relevant system operators to prepare for separation by bringing power imports and exports to zero, bringing additional generators online, and implementing other presegmentation measures. Once preparations are complete, operators could open selected breakers across BAAs nationwide to test separation operations in a controlled, relatively low-risk manner.

Contested Power Projection

Islanding could help counter China's goal of interfering with the deployment of US forces to East Asian conflict zones, and do so in ways that offer unique benefits for deterrence. In contrast to the Cold War, when US forces were heavily deployed outside the United States, the bulk of US combat capabilities are now positioned on US territory and must travel to and through US ports (sea and air) to get to future conflicts. Disrupting this flow of forces could help the PRC achieve a fait accompli in the combat zone before the bulk of US forces arrive. Creating interconnection-wide power outages would create failures across the full range of domestic transportation systems on which force projection depends and thereby help accomplish the PRC's goal.

229 DOD DSB, *Defense Science Board Task Force.*

230 ODNI, *Annual Threat Assessment*, 12.

The United States Transportation Command (USTRANSCOM) is responsible for deploying US forces in the face of such disruptions and for sustaining the flow of logistics on which those forces will depend. The commander of USTRANSCOM, Air Force Gen. Randall Reed, states that "adversaries have the ability to contest logistics across the entire spectrum, from point-of-origin to point-of-use," using both kinetic and non-kinetic disruptions that "can be just as catastrophic." The result: "we are now fighting to move, instead of moving to fight."[231]

Fighting to move will require the defense of power deliveries to a diverse array of domestic transportation systems. USTRANSCOM relies on military and commercial transportation providers for airlift and sealift as well as road and rail movements over a set of networks and nodes comprising civil highways, rail lines, seaports, airports, and operations centers, all of which need electric power to function. These assets include:

- the Strategic Highway Network (STRAHNET), which comprises over 64,200 miles of interstate and connecting highways and countless electricity-dependent traffic signals and other infrastructure;
- the Strategic Rail Corridor Network (STRACNET), which incorporates 32,000 miles of privately owned rail lines and connectors that service 141 key military installations, defense sites, and strategic seaports across the United States; and
- a Strategic Seaport Program with eighteen commercial and six military ports.[232]

As noted in the Current Fallback Defenses section, it would be extraordinarily expensive to deploy emergency generators or microgrids to sustain these assets for force projection in a blackout. If strategic power islands prove technically and politically viable, they would offer a much more cost-effective way to enable the movement of US forces to the combat zone and further contribute to the deterrence of Chinese attacks.

Implementation

Assuming that power companies can overcome the planning, technical, and operational challenges posed by strategic power islands, a further impediment would exist to adopting them as a defensive layer against cascading blackouts: the danger that grid managers will be sued by customers who lose service when islands separate from the grid and begin independent operations.

That concern may seem odd to national security officials. After all, islanding would only occur if potentially catastrophic (and life-threatening) attacks on US infrastructure were imminent or underway. But industry personnel interviewed for this study cited liability concerns as "showstopping" impediments that would need to be resolved before utilities would consider moving beyond their existing RAS, preparations for unintended islanding, and other last-ditch defense measures. Measures to indemnify the operators of strategic power islands against lawsuits will be essential to win industry support for further progress on islanding.

Liability provisions currently in place for security emergencies are woefully inadequate for such purposes. If BPS entities that comply with GSE orders "result in compliance" with NERC-approved reliability standards or other regulations, the FPA specifies that "such action or omission shall not be considered a violation of such rule, order, regulation, or provision. . . ."[233] These regulatory indemnifications *could* apply to BAs that comply with orders to island the grid.

[231] Vincent, "Transportation Command."

[232] Busler, "The Fight to Get to the Fight."

[233] 16 U.S.C. § 824o–1, (f).

Much more extensive protection would be needed to make islanding acceptable to industry. No matter how thoroughly utilities employ M&S tools to model the effects of separation and build detailed plans for island control, the initial real-world implementation of islanded operations is bound to disrupt service to some customers and prompt lawsuits for economic losses and—potentially—wrongful death.

A state-level precedent exists to indemnify BAs against such suits. State public utility commissions in California, Hawaii, and other states have adopted Public Safety Power Shutoff rules so that a utility can proactively cut power to electrical lines if it reasonably believes that strong winds may topple power lines and spark catastrophic wildfires.[234] Such power cutoffs can cause service interruptions to customers with unintended but serious effects. In 2019, for example, Pacific Gas & Electric (PG&E) implemented cutoffs to decrease the risk of its power lines igniting wildfires in parts of Northern California during extreme weather conditions. Residents and business owners subsequently sued PG&E for a total of $2.5 billion in damages. The California Supreme Court denied those claims and has enabled Public Safety Power Shutoff operations to continue under authorities that utility commissioners set in place.[235]

It would be unfair to expect ratepayers to fund such initiatives, which directly benefit national defense versus the reliability of peacetime electric service.

Congress should amend the FPA to create equivalent protections for BPS entities nationwide that comply with GSE orders, including for power islanding and other orders that may create significant interruptions of service.

Legislators should also provide funds for island development and emergency operations. The reliance of strategic power islands on existing grid infrastructure will sharply reduce their costs compared with other resilience options that require new construction. Nevertheless, for power islands that aggregate small BAAs and require new design efforts, emergency operation procedures, and staffing plans, substantial expenses could be incurred by precisely the BAs with the fewest resources to pay for them.

It would be unfair to expect ratepayers to fund such initiatives, which directly benefit national defense versus the reliability of peacetime electric service. Provisions for GSEs again provide a starting point for progress. The FPA provides that if grid operators "have incurred substantial costs to comply with an order for emergency measures issued under this subsection" and if those costs "were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners," FERC shall "establish a mechanism that permits such owners, operators, or users to recover such costs."[236]

FERC has yet to establish such a mechanism. Given rising threats to the US grid and the increasing likelihood that the secretary of energy may ultimately issue GSE orders in a future crisis, it is high time for FERC to assess policy options and criteria that enable cost recovery. Congress should expand those cost recovery provisions to federally fund BAs to plan, develop, and operate strategic power islands as well.

234 CPUC, "Public Safety Power Shutoffs."

235 Pettersson, "PG&E Ducks Negligence Suit"; and Gantner, S273340.

236 16 U.S.C. § 824o–1, (b)(6)(A).

Conclusions

The PRC is gaining new capabilities to create and sustain cascading blackouts across the three US interconnections. In response, grid operators and their government partners must not only strengthen measures to prevent cascades but also bolster fallback defenses in the event outages occur.

Building additional microgrids can help sustain service to critical loads during such blackouts. Improved AI and M&S capabilities can also help utilities manage the unintended islands that cascades and uncontrolled separation will create. Yet, if industry and government can overcome the obstacles to planning and operating strategic power islands, these islands could provide unique benefits for national security. In particular, islanding could help counter China's goals of disrupting US force projection and creating societal panic and (potentially) may be a more efficient approach than building thousands of additional microgrids or relying on luck with unintended islands.

Achieving these efficiencies may not be feasible. For excellent reasons, RCs and other BPS entities will want to continue to rely on emergency actions to prevent instabilities from spreading and do everything possible to keep interconnections up and running rather than resort to islanding. But RAS and other measures already hedge against the risk that cascades will occur. The question is whether strategic power islands can effectively supplement them. The following steps can either advance islanding initiatives or help grid operators and their partners determine that islanding is impractical or dangerous.

Island Design and Control

DOE should convene BPS entities, regulators, and state and local officials on a region-by-region basis and, using existing BAAs as a starting point and accounting for the distribution of generation resources and loads in various island configurations, examine possible island boundaries. These same partners should build on the existing roles of RCs, BAs, and other grid operators to determine how to manage islands once they separate and conduct research on how advances in data and analytics could better enable islanding on condition.

Managing Generation Shortfalls

Despite efforts to optimize island boundaries to facilitate balancing, some islands will lack sufficient generation to service all of their loads. Prospective island managers should use existing load-shedding plans to identify priorities to sustain power to hospitals and other civilian facilities vital for public health and safety. Emergency managers and state and local government officials should also strengthen existing disaster response plans and capabilities to limit casualties in the event of extended wartime contingencies.

To enable the execution of DOW missions, including those necessary to support the dispersed and interdependent infrastructure necessary for fort-to-port operations, the assistant secretary of war for homeland defense and hemispheric affairs, the Joint Staff, and other DOW organizations should identify the facilities and functions that will require power within specific islands. With the help of DOE, those data should then be securely shared with island managers so they can prioritize electric service to such mission-critical loads.

Island Separation

DOE should convene RCs and BPS entities to further examine the risks and benefits of islanding on condition versus on warning. In doing so, they should account for the possibility that if the IC believes a Chinese attack is imminent, the president will declare a GSE and the secretary of energy will issue orders to protect the grid from cascading blackouts. The best way to ensure that these orders are helpful is for DOE to collaborate with industry to develop them. Such consultative efforts should begin immediately.

Island Resilience

FERC, NERC, and their industry partners should continue to strengthen cyber and physical security measures so that islands can survive once they separate from the grid. Resilience against UAS attacks should be a particular priority and will require action by Congress and the Federal Aviation Administration to facilitate the defense of critical substations and other assets. In addition, the managers of natural gas–dependent islands should develop contingency plans for gas shortages, including for even more stringent load shedding and prioritization measures in case generation is severely disrupted.

Implementation

Congress should indemnify island managers against the economic damage and loss of life that separation is likely to entail. Legislators will also need to fund the M&S work and other activities necessary to plan for islanding given that these efforts directly benefit the common defense versus peacetime reliability of service for ratepayers.

Deterrence

The ability to island and sustain service to critical loads, especially those that Chinese leaders most hope to disrupt, is necessary but not sufficient to strengthen deterrence. The United States must also convince those leaders that islanding will be effective and thereby reduce their confidence that they can achieve their goals in attacking the grid at a cost they consider acceptable. Industry should partner with DOE to conduct exercises, targeted messaging campaigns, and other initiatives to influence Xi Jinping's calculations and thereby help achieve the greatest potential benefit of islanding: reducing the likelihood that China will attack.

Bibliography

American Water. *2022 Annual Water Quality Report*. https://www.amwater.com/ccr/forthood.pdf.

Anthropic. *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign*. Anthropic, November 2025. https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.

Anthropic. *Project Glasswing: Securing Critical Software for the AI Era.* April 7, 2026. https://www.anthropic.com/glasswing.

Anvari, Mehrnaz, and Thomas Vogt. "Identifying the Power-Grid Bottlenecks Responsible for Cascading Failures During Extreme Storms." *Nature Energy* 9 (2024): 516–517. https://www.nature.com/articles/s41560-024-01499-6.

Behr, Peter. "Spain's Big Blackout: A Cautionary Tale for US Grid Managers." *E&E News*, June 27, 2025. https://www.eenews.net/articles/spains-big-blackout-a-cautionary-tale-for-us-grid-managers/.

Biswas, Shuchismita, Jim Follum, Eric Andersen, and Jeffery S. Banning. *Big Data Analysis of Synchrophasor Data*. Richland, WA: Pacific Northwest National Laboratory, October 13, 2022. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-33548.pdf.

Booth, Samuel, James Reilly, Robert Butt, Mick Wasco, and Randy Monohan. *Microgrids for Energy Resilience: A Guide to Conceptual Design and Lessons from Defense Projects*. Golden, CO: National Renewable Energy Laboratory (2020). https://docs.nlr.gov/docs/fy19osti/72586.pdf.

Brumfield, Cynthia. "Ignoring AI in the Threat Chain Could Be a Costly Mistake, Experts Warn." *CSO Online*, December 9, 2025. https://www.csoonline.com/article/4101936/ignoring-ai-in-the-threat-chain-could-be-a-costly-mistake-experts-warn.html.

Buchele, Mose, and Matt Largey. "If the Texas Power Grid Had Gone Down, It Would Need a 'Black Start.' How Long Would That Take?" *KUT News*, August 5, 2021. https://www.kut.org/energy-environment/2021-08-05/if-the-texas-power-grid-had-gone-down-it-would-need-a-black-start-how-long-would-that-take.

Burger, Andrew. "A $100 Million Microgrid Proposed for Downtown Cleveland." *Microgrid Knowledge*, October 25, 2018. https://www.microgridknowledge.com/microgrids/commercial/article/11430147/a-100-million-microgrid-proposed-for-downtown-cleveland.

Busler, Bruce. "The Fight to Get to the Fight: Deploying from a Contested Homeland." *DTJ Online*, October 3, 2024. https://www.ndtahq.com/the-fight-to-get-to-the-fight-deploying-from-a-contested-homeland/.

Buttel, Lindsey. "America's Electricity Generation Capacity, 2025 Update." American Public Power Association, April 2025. https://www.publicpower.org/system/files/documents/Americas-Electricity-Generation-Capacity-2025-Update.pdf.

CAISO (California Independent System Operator). "Balancing Authority." https://www.caiso.com/about/our-business/balancing-authority.

———. *Root Cause Analysis: Mid-August 2020 Extreme Heat Wave.* January 13, 2021. https://www.caiso.com/Documents/Final-Root-Cause-Analysis-Mid-August-2020-Extreme-Heat-Wave.pdf.

California Energy Commission. "Balancing Authority Areas: California 2020." https://gis.data.ca.gov/documents/07c4d7253138472782716db5ff4cf62a/explore.

———. "2024 Total System Electric Generation." https://www.energy.ca.gov/data-reports/energy-almanac/california-electricity-data/2024-total-system-electric-generation.

Chapman, Ben. "LAPD Secures $9.8 Million DHS Grant to Protects City's Airspace From Drones." *New York Post*, February 24, 2026. https://nypost.com/2026/02/24/us-news/los-angeles-police-department-approved-a-9-8-million-dhs-grant-for-anti-drone-technology/.

Chen, Chao-Yang, Yang Zhao, Jianxi Gao, and Harry Eugene Stanley. "Nonlinear Model of Cascade Failure in Weighted Complex Networks Considering Overloaded Edges." *Scientific Reports* 10 (2020): 13428. https://doi.org/10.1038/s41598-020-69775-5.

Chen, Yousu, Xiaoyuan Fan, Renke Huang, Qiuhua Huang, Ang Li, and Kishan Guddanti. *Artificial Intelligence/Machine Learning Technology in Power System Applications*. Richland, WA: Pacific Northwest National Laboratory, March 2024. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-35735.pdf.

Chivers, C. J. "In Ukraine, a New Arsenal of Killer A.I. Drones Is Being Born." *New York Times*, December 31, 2025. https://www.nytimes.com/2025/12/31/magazine/ukraine-ai-drones-war-russia.html.

CISA (Cybersecurity and Infrastructure Security Agency). "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." February 7, 2004. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

———. "Regional Resiliency Assessment Program." June 8, 2023. https://www.cisa.gov/sites/default/files/2023-06/Regional%20Resiliency%20Assessment%20Program%20%28RRAP%29%20Fact%20Sheet%202023.pdf.

———. "Release Cybersecurity Guidance on Chinese-Manufactured UAS for Critical Infrastructure Owners and Operators." News release, January 17, 2024. https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators.

City of Norfolk. "City of Norfolk Utilities." https://www.norfolk.gov/DocumentCenter/View/74743/Utilities-Pamphlet.

Clark, Corrie E. *Electric Reliability and Resiliency in Puerto Rico*. In Focus IF 12913. Washington, DC: Congressional Research Service, May 30, 2025. https://www.congress.gov/crs-product/IF12913.

Collett-White, Mike, Prasanta Kumar Dutta, and Mariano Zafra. "How Ukraine Pulled Off an Audacious Attack Deep Inside Russia." *Reuters*, June 4, 2025. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES-RUSSIA/mypmjzayyvr/.

Cox, Matthew. "Many US Bases Still Lack Sufficient Tech to Track Drone Incursions: DOD Officials." *Air & Space Forces Magazine*, April 29, 2025. https://www.airandspaceforces.com/many-us-bases-still-lack-sufficient-tech-to-track-drone-incursions-dod-officials/.

CPUC (California Public Utilities Commission). "Public Safety Power Shutoffs (PSPS)." https://www.cpuc.ca.gov/psps/.

C2ES (Center for Climate and Energy Solutions). "Microgrids." https://www.c2es.org/content/microgrids/.

Danzig, Richard. *Artificial Intelligence, Cybersecurity, and National Security: The Fierce Urgency of Now*. Santa Monica, CA: RAND Corporation, July 14, 2025. https://www.rand.org/pubs/perspectives/PEA4079-1.html.

Dashevskyi, Stanislav, Francesco La Spina, and Daniel dos Santos. *SUN:DOWN: Destabilizing the Grid via Orchestrated Exploitation of Soar Power Systems*. Forescout Research, March 27, 2025. https://www.forescout.com/resources/sun-down-research-report/.

DC Water. *Approved FY 2024 Budgets, Section II: Overview*. March 2, 2023. https://www.dcwater.com/sites/default/files/finance/budgets/2024/Approved%20FY%202024_Section%20II_Budget%20Overview.pdf.

Deeks, Ashley, and Madison Rinder. "Are Domestic Drone Shoot-Downs Lawful?" *Lawfare*, February 5, 2025. https://www.lawfaremedia.org/article/are-domestic-drone-shoot-downs-lawful.

Deming, Robby. "Grids and Generators: Energy Production and Distribution in the US." Maps.com, October 27, 2025. https://www.maps.com/us-energy-map-reveals-grid-and-energy-sources/.

Denholm, P., and J. Cochran. *Balancing Area Coordination: Efficiently Integrating Renewable Energy into the Grid*. https://docs.nlr.gov/docs/fy15osti/63037.pdf.

DHS (US Department of Homeland Security). "Counter-Unmanned Aerial Systems (C-UAS) Grant Program." October 30, 2025. https://sam.gov/fal/f6d30faaaf2942f5b148db296c0c8287/view#history.

Dizikes, Peter. "What's the Best Way to Expand the US Electricity Grid?" *MIT News*, December 4, 2025. https://news.mit.edu/2025/best-way-to-expand-us-electricity-grid-1204.

DOD (US Department of Defense). "FACT SHEET: Department of Defense Strategy for Countering Unmanned Systems." December 2024. https://media.defense.gov/2024/Dec/05/2003599149/-1/-1/0/FACT-SHEET-STRATEGY-FOR-COUNTERING-UNMANNED-SYSTEMS.PDF.

———. *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress*. Washington, DC: DOD, 2024. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

DOD DSB (US Department of Defense Defense Science Board). *Department of Defense Dependencies on Critical Infrastructure*. Washington, DC: DOD DSB, August 2024. https://dsb.cto.mil/wp-content/uploads/2024/10/DSB_CriticalInfrastructure_ExecutiveSummary.pdf.

———. *Defense Science Board Task Force on Cyber Deterrence*. February 2017. https://apps.dtic.mil/sti/pdfs/AD1028516.pdf.

DOE (US Department of Energy). "Achieving American Leadership in the Electric Grid Supply Chain." February 24, 2022. https://www.energy.gov/sites/default/files/2024-12/Electric%2520Grid%2520Supply%2520Chain%2520Fact%2520Sheet%5B1%5D.pdf.

———. "Addressing Security and Reliability Concerns of Large Power Transformers." https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers.

———. *Distribution Standard of Conduct*. November 2023. https://www.energy.gov/sites/default/files/2023-11/2023-11-01%20Distribution%20Standard%20of%20Conduct%20nov%202023_optimized_0.pdf.

———. "DOE's Use of Federal Power Act Emergency Authority." https://www.energy.gov/ceser/does-use-federal-power-act-emergency-authority.

———. "Energy Department Announces $625 Million Investment to Reinvigorate and Expand America's Coal Industry." September 29, 2025. https://www.energy.gov/articles/energy-department-announces-625-million-investment-reinvigorate-and-expand-americas-coal.

———. "Grid Security Emergency Orders: Procedures for Issuance." *Federal Register* 83, no. 7 (January 10, 2018). https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance.

———. "How It Works: The Role of a Balancing Authority." https://www.energy.gov/sites/default/files/2023-08/Balancing%20Authority%20Backgrounder_2022-Formatted_041723_508.pdf.

———. *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 Interest Electric Transmission Corridor Designation Process." https://www.energy.gov/gdo/national-interest-electric-transmission-corridor-designation-process.

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

———. "Practicing Defense and Resilience at Liberty Eclipse." January 9, 2024. https://www.energy.gov/ceser/articles/practicing-defense-and-resilience-liberty-eclipse.

———. *Resource Adequacy Report: Evaluating the Reliability and Security of the United States Electric Grid*. July 2025. https://www.energy.gov/sites/default/files/2025-07/DOE%20Final%20EO%20Report%20%28FINAL%20JULY%207%29.pdf.

———. "Speed to Power Initiative." https://www.energy.gov/speed-to-power.

———. *TSO-DSO-Aggregator Market and Operational Coordination Requirements*. April 2024. https://www.energy.gov/sites/default/files/2024-07/47990_DOE_OE_TDC_Project_Coordination_Platform_v9_RELEASE_508.pdf.

DOE GDO (US Department of Energy Grid Deployment Office). *Territory of Guam*. June 2024. https://www.energy.gov/sites/default/files/2024-10/TerritorySectorRiskProfile-Guam.pdf.

DOJ (US Department of Justice). "Man Pleads Guilty to Attempting to Use a Weapon of Mass Destruction and Attempting to Destroy an Energy Facility in Nashville." Press release, September 9, 2025. https://www.justice.gov/opa/pr/man-pleads-guilty-attempting-use-weapon-mass-destruction-and-attempting-destroy-energy.

DOW (US Department of War). "JIATF-401 Announces Updated Guidance to Counter Drone Threats in the Homeland." Release, January 26, 2026. https://www.war.gov/News/Releases/Release/Article/4389392/jiatf-401-announces-updated-guidance-to-counter-drone-threats-in-the-homeland/.

———. *2025 Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*. December 2025. https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.

EEI (Edison Electric Institute). *EEI Emergency Response Programs and Playbooks*. June 2021. https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Reliability-and-Emergency-Response/EmergencyResponse_Programs_Playbooks.pdf.

———. *Spare Equipment and Grid Resilience*. August 1, 2023. https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Reliability-and-Emergency-Response/Spare-Equipment-and-Grid-Resilience-Programs.pdf.

EIA (US Energy Information Administration). "About 25% of U.S. Power Plants Can Start Up Within an Hour." November 19, 2020. https://www.eia.gov/todayinenergy/detail.php?id=45956.

———. "California Overview." https://www.eia.gov/state/print.php?sid=CA.

———. "California Was the Largest Net Electricity Importer of Any State in 2019." December 7, 2020. https://www.eia.gov/todayinenergy/detail.php?id=46156.

———. "District of Columbia Analysis." March 19, 2026. https://www.eia.gov/state/analysis.php?sid=DC.

———. "Hourly Electric Grid Monitor." https://www.eia.gov/electricity/gridmonitor/about.

———. "How Many Power Plants Are in the United States?" October 20, 2023. https://www.eia.gov/tools/faqs/faq.php?id=65&t=2.

———. "U.S. Developers Report Half of New Electric Generating Capacity Will Come from Solar." August 20, 2025. https://www.eia.gov/todayinenergy/detail.php?id=65964.

———. "U.S. Electricity Exports to Canada Have Increased Since September 2023." March 6, 2025. https://www.eia.gov/todayinenergy/detail.php?id=63684.

———. "US Electric System Is Made Up of Interconnections and Balancing Authorities." July 20, 2016. https://www.eia.gov/todayinenergy/detail.php?id=27152.

———. "What Is U.S. Electricity Generation by Energy Source?" February 2024. https://www.eia.gov/tools/faqs/faq.php?id=427&t=3.

e-Magic. "The Silent Power Crisis: How IoT-Driven Digital Twins Could Prevent the Next Blackout." Blog post, June 9, 2025. https://www.e-magic.ca/post/the-silent-power-crisis-how-iot-driven-digital-twins-could-prevent-the-next-blackout.

Enriquez-Contreras, Luis Fernando, S M Shafiul Alam, Timothy R. McJunkin, Megan Culler, Jonathan Tacke, and Emma Stewart. *MegaWatt Mayhem: Grid Operator Challenges with Large Loads*. Idaho Falls, ID: Idaho National Laboratory, September 2025. https://csdet.inl.gov/content/uploads/45/2025/10/MegaWatt_Mayhem.pdf.

EPA (Environmental Protection Agency). "Information about Public Water Systems." https://www.epa.gov/dwreginfo/information-about-public-water-systems.

———. *Power Resilience: Guide for Water and Wastewater Utilities*. June 2019. https://www.epa.gov/sites/default/files/2016-03/documents/160212-powerresilienceguide508.pdf.

EPRI (Electric Power Research Institute). *SOLAr Critical Infrastructure Energization (SOLACE): Leveraging Distributed Energy Resources to Provide Local Power*. Palo Alto, CA: EPRI, 2023. https://www.epri.com/research/programs/067418/results/3002026254.

———. *Use Case 14 – Controlled Islanding.* https://smartgrid.epri.com/usecases/controlledislanding.pdf.

ERCOT. *ERCOT Nodal Operating Guides, Section 4: Emergency Operation*. August 1, 2025. https://www.ercot.com/files/docs/2022/05/27/04-080125.doc.

ESCC (Electricity Subsector Coordinating Council). ESCC Brochure. March 2026. https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure.

Evron, Gadi, Rich Mogull, and Rob T. Lee. *The "AI Vulnerability Storm": Building a "Mythos-Ready" Security Program.* Cloud Security Alliance, April 12, 2026. https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/04/mythosready-20260413.pdf.

FCC (Federal Communications Commission). "FACT SHEET: FCC Updates Covered List to Include Foreign UAS and UAS Critical Components on Going Forward Basis." December 22, 2025. https://docs.fcc.gov/public/attachments/DOC-416839A1.pdf.

Federal Power Commission. *Northeast Power Failure, November 9 and 10, 1965: A Report to the President by the Federal Power Commission.* Washington, DC: Government Printing Office, December 1965. https://books.google.com/books?id=dUNSAQAAIAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

FERC (Federal Energy Regulatory Commission). *Blackstart and Next-Start Resource Availability in the Texas Interconnection: FERC, NERC, and Regional Entity Staff Study*. December 2023. https://www.ferc.gov/media/ferc-nerc-regional-entity-joint-blackstart-and-next-start-resource-availability-study-texas.

———. *The February 2021 Cold Weather Outages in Texas and South Central United States: FERC, NERC and Regional Entity Staff Report*. December 8, 2021. https://www.ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and.

———. *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.

———. *Improvements to Generator Interconnection Procedures and Agreements*. Order No. 2023. 184 FERC ¶ 61,054. July 28, 2023. https://www.ferc.gov/media/order-no-2023.

———. *Reliability Primer*. Washington, DC: FERC, 2016. https://www.ferc.gov/sites/default/files/2020-04/reliability-primer_1.pdf.

———. "RTOs and ISOs." https://www.ferc.gov/power-sales-and-markets/rtos-and-isos.

FERC and NERC (Federal Energy Regulatory Commission and North American Electric Reliability Corporation). *Arizona-Southern California Outages on September 8, 2011: Causes and Recommendations*. April 2012. https://www.nerc.com/pa/rrm/ea/Documents/AZOutage_Report_01MAY12.pdf.

15 U.S.C. § 9401. https://uscode.house.gov/view.xhtml?req=(title:15%20section:9401%20edition:prelim).

Fuzaylov, Ariella. "Why Transmission Congestion Matters in the Energy Transition." Synapse Energy Economics, February 27, 2025. https://www.synapse-energy.com/why-transmission-congestion-matters-energy-transition#:~:text=Congestion%20occurs%20on%20the%20transmission,a%20bottleneck%20in%20the%20system.

Gantner v. PG&E Corp. S273340 (Cal. Nov. 20, 2023). https://law.justia.com/cases/california/supreme-court/2023/s273340.html.

Giraldez, Julieta, Francisco Flores-Espino, Sara MacAlpine, and Peter Asmus. *Phase I Microgrid Cost Study: Data Collection and Analysis of Microgrid Costs in the United States*. Golden, CO: National Renewable Energy Laboratory, October 2018. https://docs.nlr.gov/docs/fy19osti/67821.pdf.

Gracia, Jose R., Lawrence C. Markel, D. Thomas Rizy, Patrick W. O'Connor, Rui Shan, and Alfonso Tarditi. *Hydropower Plants as Black Start Resources*. May 2019. https://www.energy.gov/sites/prod/files/2019/05/f62/Hydro-Black-Start_May2019.pdf.

Halper, Evan, and Ellen Nakashima. "This One Gadget Could Give China a Back Door into the U.S. Power Grid." *Washington Post*, December 10, 2025. https://www.washingtonpost.com/business/2025/12/10/us-energy-grid-china-threat-blackouts/.

Hansen, Chris. "La Plata Electric CEO: Why Western Utilities Are Moving toward Regional Markets." *Utility Dive*, April 20, 2026.

Hashemi, Sina, Balaji V. Venkatasubramanian, Pierluigi Mancarella, and Mathaios Panteli. "Cascading-Driven Intentional Controlled Islanding for Enhancing Power Grid Operational Resilience." *Journal of Modern Power Systems and Clean Energy* 14, no. 2 (2026): 514–528. https://doi.org/10.35833/MPCE.2024.001371.

Hassani Ahangar, Amir Reza, Gevork B. Gharehpetian, and Hamid Reza Baghaee. "A Review on Intentional Controlled Islanding in Smart Power Systems and Generalized Framework for ICI in Microgrids." *International Journal of Electrical Power & Energy Systems* 118 (2020): 105709. https://doi.org/10.1016/j.ijepes.2019.105709.

Hayat, Faisal, Muhammad Adnan, Muhammad Sajid Iqbal, Salah Eldeen Gasim Mohamed, and Muhammad Tariq. “Expert and Intelligent Systems for Assessment and Mitigation of Cascading Failures in Smart Grids: Research Challenges and Survey.” *Results in Engineering* 28 (2025): 107148, https://doi.org/10.1016/j.rineng.2025.107148.

Hitchens, Kathy. “Yokota Air Base Celebrates the Completion of Its New Microgrid.” *Microgrid Knowledge*, November 1, 2023. https://www.microgridknowledge.com/military-microgrids/article/33014051/yokota-air-base-celebrates-the-completion-of-its-new-microgrid.

Howland, Ethan. “NERC President Warns of ‘Five-Alarm Fire’ for Grid Reliability.” *Utility Dive*, October 22, 2025. https://www.utilitydive.com/news/data-center-grid-reliability-ferc-nerc/803467/.

IARC (International Arctic Research Center). “Alaska’s Arctic Energy System.” https://uaf-iarc.org/alaska-arctic-policy-trends/energy-issues/arctic-energy/.

ICS Investigation Expert Panel. *Final Report: Grid Incident in Spain and Portugal on 28 April 2025*. March 20, 2026. https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Publications/2025/iberian-blackout/Final%20Report%20on%20the%20Grid%20Incident%20in%20Spain%20and%20Portugal%20on%2028%20April%202025.pdf.

Kramer, Franklin, Robert Butler, and Melanie Teplinsky. “Defeating the Cyber Invasion with a National Cyber Force.” *The Cyber Defense Review* 11, no. 1 (2026). https://cyberdefensereview.army.mil/Portals/6/Documents/2026-in-press/CDR_IP_Kramer_Butler_Teplinsky_SLP.pdf.

Kroposki, Ben. “Prevention of Unintentional Islands in Power Systems with Distributed Resources.” Webinar presentation, August 24, 2016. https://www.nlr.gov/grid/ieee-standard-1547/prevention-unintentional-islands.

Langerová, Erika. “China Is Studying How to Hack and Crash Our Power Grids.” *Homeland Security Today*, July 9, 2025. https://www.hstoday.us/subject-matter-areas/cybersecurity/china-is-studying-how-to-hack-and-crash-our-power-grids/.

Lauby, Mark. “Iberian Peninsula Blackout: Contextual Comparison with North American BPS Reliability Safeguards.” FERC Open Meeting presentation, June 26, 2025. https://www.ferc.gov/sites/default/files/2025-06/Iberian%20Peninsula%20Blackout%20April%202025_final.pdf.

Levitan and Associates. *Northeast Gas/Electric System Study*. Boston: Levitan and Associates, January 21, 2025. https://cdn.prod.website-files.com/67229043316834b1a60feba3/678fee912264907c381a0f68_NPCC%20Northeast%20Gas%20Electric%20System%20Study.pdf.

Margolin, Josh, and Aaron Katersky. “‘Multiple Waves’ of Unauthorized Drones Recently Spotted Over Strategic US Air Force Base.” *ABC News*, March 20, 2026. https://abcnews.com/International/multiple-waves-unauthorized-drones-spotted-strategic-us-air/story?id=131245527.

Meissner, Brad. “AI and Microgrids: Moving Toward Seamless, Resilient Energy Solutions.” *Utility Dive*, May 28, 2025. https://www.utilitydive.com/news/ai-microgrids-resilient-energy-solutions-generac/749121/.

Michigan Public Service Commission. *Report on the August 14th Blackout*. November 2003. https://www.michigan.gov/-/media/Project/Websites/mpsc/regulatory/reports/mpsc_blackout.pdf.

Narang, David, Sigifredo Gonzalez, Michael Ingram, and Michael Ropp. *Overview of Functional Technical Requirements for Intentional Islands*. Golden, CO: National Renewable Energy Laboratory, December 2022. https://docs.nlr.gov/docs/fy23osti/83301.pdf.

NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity Baselines for Electric Distribution Systems and DER*. February 2024. https://www.energy.gov/sites/default/files/2025-01/NARUC_Cybersecurity-Baselines-Report%201.pdf.

NASEM (National Academies of Sciences, Engineering, and Medicine). *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: The National Academies Press, 2017.

NATF (North American Transmission Forum). *Bulk Electric Systems Operations Absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach*. 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.

NERC (North American Electric Reliability Corporation). *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-005-1—Balancing Authority Control*. Atlanta: NERC, September 20, 2017. https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-005-1.pdf.

———. *BAL-003-2—Frequency Response and Frequency Bias Setting*. Atlanta: NERC. https://www.nerc.com/pa/stand/reliability%20standards/bal-003-2.pdf.

———. *Characteristics and Risks of Emerging Large Loads*. Atlanta: NERC, July 2025. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Whitepaper%20Characteristics%20and%20Risks%20of%20Emerging%20Large%20Loads.pdf.

———. *CIP-014-3—Physical Security*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf.

———. *CIP-008-7—Cyber Security — Incident Reporting and Response Planning*. Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-008-7.pdf.

———. *Draft Security Guideline: Risk Assessments and Voluntary Physical Security Protection Best Practices at Non-Critical Bulk Power System Facilities*. Atlanta: NERC, September 2025. https://www.nerc.com/comm/RSTCReviewItems/1_09_SG_Risk_Assessments_and_Best_Practices_at_non-Critical_BPS_Facilities.pdf.

———. *EOP-008-2—Loss of Control Center Functionality*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-008-2.pdf.

———. *EOP-011-4—Emergency Operations*. Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/eop/eop-011-4.pdf.

———. *EOP-005-3—System Restoration from Blackstart Resources*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-005-3.pdf.

———. *EOP-006-3—System Restoration Coordination*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-006-3.pdf.

———. *EOP-002-3.1—Capacity and Energy Emergencies*. Atlanta: NERC, March 2014. https://www.nerc.com/globalassets/programs/compliance/rsaws/rsaw-eop-002-3.1_march_-2014.docx.

———. *ERO Enterprise Joint IROL Activity Report*. Atlanta: NERC, July 2024. https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20Enterprise%20Joint%20IROL%20Activity%20Report%20-%20July%202024.pdf.

———. *Glossary of Terms Used in NERC Reliability Standards.* Atlanta: NERC, November 5, 2025. https://www.nerc.com/globalassets/standards/reliability-standards/glossary_of_terms.pdf.

———. *Incident Review: Voltage-Sensitive Crypto Load Reductions*. Atlanta: NERC, January 9, 2026. https://www.nerc.com/globalassets/our-work/reports/event-reports/incident_review_considering_voltage-sensitive_crypto_load_reductions.pdf.

———. *Interregional Transfer Capability Study (ITCS): Strengthening Reliability through the Energy Transformation*. Atlanta: NERC, November 2024. https://www.nerc.com/pa/RAPA/Documents/ITCS_Final_Report.pdf.

———. *IRO-008-3—Reliability Coordinator Operational Analyses and Real-time Assessments*. Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/iro/iro-008-3.pdf.

———. *IRO-009-2—Reliability Coordinator Actions to Operate within IROLs*. Atlanta: NERC, December 4, 2015. https://www.nerc.com/globalassets/standards/reliability-standards/iro/iro-009-2.pdf.

———. *IRO-002-7— Reliability Coordination – Monitoring and Analysis*. Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/iro/iro-002-7.pdf.

———. *Long-Term Reliability Assessment*. Atlanta: NERC, January 2026. https://www.nerc.com/globalassets/our-work/assessments/nerc_ltra_2025.pdf.

———. *PRC-012-2—Remedial Action Schemes*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-012-2.pdf.

———. *PRC-024-4—Frequency and Voltage Protection Settings for Synchronous Generators, Type 1 and Type 2 Wind Resources, and Synchronous Condensers.* Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-024-4.pdf.

———. *PRC-024-3—Frequency and Voltage Protection Settings for Generating Resources.* Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-024-3.pdf.

———. *PRC-024-2—Generator Frequency and Voltage Protective Relay Settings.* Atlanta: NERC. https://www.nerc.com/globalassets/standards/projects/2014-01/prc-024-2_clean_2015_jan_12.pdf.

———. *PRC-029-1—Frequency and Voltage Ride-through Requirements for Inverter-based Resources*. Atlanta: NERC. https://www.nerc.com/standards/reliability-standards/prc/prc-029-1.

———. *PRC-027-1—Coordination of Protection Systems for Performance during Faults.* Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-027-1.pdf.

———. *PRC-026-2—Relay Performance during Stable Power Swings.* Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-026-2.pdf.

———. *PRC-030-1—Unexpected Inverter-Based Resource Event Mitigation*. Atlanta: NERC. https://www.nerc.com/standards/reliability-standards/prc/prc-030-1.

———. *PRC-006-NPCC-2—Automatic Underfrequency Load Shedding*. Atlanta: NERC. https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-006-NPCC-2.pdf.

———. *PRC-006-5—Automatic Underfrequency Load Shedding*. Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-006-5.pdf.

———. "Project 2023-06 CIP-014 Risk Assessment Refinement." Atlanta: NERC. https://www.nerc.com/pa/Stand/Pages/Project_2023-06_CIP-014_Risk_Assessment_Refinement.aspx.

———. *Reliability Guideline: Methods for Establishing IROLs*. Atlanta: NERC, September 2018. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf.

———. *Reliability Issues Steering Committee: Report on Resilience*. Atlanta: NERC, November 8, 2018. https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20Resilience%20Report_Approved_RISC_Committee_November_8_2018_Board_Accepted.pdf.

———. *Severe Impact Resilience: Considerations and Recommendations*. Atlanta: NERC, May 9, 2012. https://www.ourenergypolicy.org/wp-content/uploads/2012/05/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

———. *Transmission and Distribution Coordination Strategies*. SPIDERWG White Paper. Atlanta: NERC, October 2023. https://www.nerc.com/globalassets/our-work/white-papers/tanddcoordinationdocument_draft_white_paper.pdf.

———. *TOP-001-6—Transmission Operations*. Atlanta: NERC. https://www.nerc.com/globalassets/standards/reliability-standards/top/top-001-6.pdf.

———. *2025 ERO Reliability Risk Priorities Report*. Atlanta: NERC, August 14, 2025. https://www.nerc.com/globalassets/our-work/reports/ero-reliability-risk-priorities-report/2025_risc_ero_priorities_report.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.

———. "Who We Are." https://www.nerc.com/who-we-are.

NREL (National Renewable Energy Laboratory). *Absorbing the Sun: Operational Practices and Balancing Reserves in Florida's Municipal Utilities*. Golden, CO: NREL (2021). https://docs.nlr.gov/docs/fy21osti/78306.pdf.

NSCAI (National Security Commission on Artificial Intelligence). *Final Report*. Washington, DC: NSCAI, March 19, 2021.

Nuclear Regulatory Commission. "Station Blackout." *Federal Register* 77, no. 54 (2012): 16175. https://www.federalregister.gov/documents/2012/03/20/2012-6665/station-blackout.

NWPCC (Northwest Power and Conservation Council). "Blackout of 1996." https://www.nwcouncil.org/reports/columbia-river-history/blackout/.

ODNI (Office of the Director of National Intelligence). *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: ODNI, March 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

———. *2026 Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: ODNI, March 2026. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf.

OUSW(C) (Office of the Under Secretary of War, Comptroller). *FY 2024 Energy Resilience and Conservation Investment Program (ERCIP)*. March 2023. https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/07_Military_Construction/15-Energy_Resilience_and_Conservation_Investment_Program.pdf.

Pettersson, Edvard. "PG&E Ducks Negligence Suit over Wildfire Prevention Shutoffs." *Courthouse News Service*, November 20, 2023. https://www.courthousenews.com/pge-ducks-negligence-suit-over-wildfire-prevention-shutoffs/.

Pitts, Russell. "Force Protection Conditions – A Tutorial." Defense Logistics Agency, August 20, 2021. https://www.dla.mil/About-DLA/News/News-Article-View/Article/2740252/force-protection-conditions-a-tutorial/.

PJM. "PJM – At a Glance." Fact Sheet. https://www.pjm.com/-/media/DotCom/about-pjm/newsroom/fact-sheets/pjm-at-a-glance.pdf.

———. "PJM Publishes 2024 Long-Term Load Forecast." *PJM Inside Lines*, January 8, 2024. https://insidelines.pjm.com/pjm-publishes-2024-long-term-load-forecast/.

PNNL (Pacific Northwest National Laboratory). "Transformative Remedial Action Scheme Tool (TRAST)." September 2019. https://www.pnnl.gov/sites/default/files/media/file/DDST_0066_FLIER_AISummit_TRAST_WEB.pdf.

Pomerleau, Mark. "DOD Creating Joint Interagency Counter-Drone Task Force." *DefenseScoop*, July 2, 2025. https://defensescoop.com/2025/07/02/dod-creating-joint-interagency-counter-drone-task-force-gen-mingus/.

Power Struggle: Examining the 2021 Texas Grid Failure, before the Oversight and Investigations Subcommittee of House Energy and Commerce Committee, 117th Cong. (March 24, 2021) (statement of Bill Magness, President and Chief Executive Officer of the Electric Reliability Council of Texas).

Quint, Ryan, Andrew Isaacs, Farhad Yahyaie, Lukas Unruh, Julia Matevosyan, and Casey Baker. *A Call to Action for a Stable Energy Transition: Grid-Forming Battery Energy Storage Systems*. Energy Systems Integration Group, March 2025. https://www.esig.energy/wp-content/uploads/2025/03/ESIG-GFM-BESS-brief-2025.pdf.

RFL. "Remedial Action Scheme/Special Protection Schemes Solutions." https://www.rflelect.com/solutions/protective-relaying-communications-solutions/remedial-action-scheme-special-protection-schemes-solutions.

Roose, Kevin. "Anthropic Claims Its New A.I. Model, Mythos, Is a Cybersecurity 'Reckoning.'" *New York Times*, April 7, 2026. https://www.nytimes.com/2026/04/07/technology/anthropic-claims-its-new-ai-model-mythos-is-a-cybersecurity-reckoning.html.

RRC (Railbelt Reliability Council). "About the RCC." https://www.akrrc.org/about-rrc.

Senga, Juan Ramon L., Audun Botterud, John E. Parsons, S. Drew Story, and Christopher R. Knittel. "Implications of Policy-Driven Transmission Expansion for Costs, Emissions and Reliability in the USA." *Nature Energy* 11 (2026): 230–243. https://doi.org/10.1038/s41560-025-01921-7.

SERC Reliability Corporation. *Guideline: Conservative Operations*. September 23, 2020. https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-guideline_rev-1-03-21-17.pdf?sfvrsn=2.

Simeone, Christina E., and Amy Rose. *Barriers and Opportunities to Realize the System Value of Interregional Transmission*. Golden, CO: National Renewable Energy Laboratory, June 2024.

Singh, Ishveena. "DJI Pushes Massive Firmware Update across Enterprise Drone Ecosystem." Drone DJ, December 15, 2025. https://dronedj.com/2025/12/15/dji-enterprise-drone-dock-firmware/.

16 U.S.C. § 824o–1. https://www.govinfo.gov/content/pkg/USCODE-2024-title16/pdf/USCODE-2024-title16-chap12-subchapII-sec824o-1.pdf.

SPP (Southwest Power Pool). *SPP BA Emergency Operating Plan V10.* August 21, 2025. https://spp.org/documents/74612/spp%20ba%20emergency%20operating%20plan_v%2010.0%20-%20redline.pdf.

———. *2026 RTO Expansion SWPW Transition Plan*. March 1, 2026. https://spp.org/documents/75997/2026%20rtoe%20swpw%20transition%20plan%20%E2%80%93%20market%20participant.pdf.

State of Hawaii Public Utilities Commission. "Resilience and Reliability." https://puc.hawaii.gov/hazard-mitigation-resilience-and-recovery/resilience-and-reliability/.

Stockton, Paul. *Electric Infrastructure Protection (EPRO®) Handbook II: Volume 1—Fuel.* Washington, DC: Electric Infrastructure Security Council, 2016.

———. *Surfing the Wave: Resilience Strategies for the Decentralizing Grid*. Laurel, MD: Johns Hopkins Applied Physics Laboratory, 2025. https://www.jhuapl.edu/sites/default/files/2025-03/SurfingTheWave-WEB.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.

Striderintel.com. *In Broad Daylight: U.S. Grid Exposed to Risk from PRC-Made Inverter Equipment.* Strider, November 2025. https://content.striderintel.com/wp-content/uploads/2025/11/Strider-Report-In-Broad-Daylight-2025.pdf.

Sytas, Andrius, and Marek Strzelecki. "On NATO's Eastern Flank, Bunkers and Anti-Drone Nets Set to Protect Power Grids." *Reuters*, September 29, 2025. https://www.reuters.com/business/energy/natos-eastern-flank-bunkers-anti-drone-nets-set-protect-power-grids-2025-09-29/.

Tang, Fei, Yuhan Guo, Xiaoqing Wei, Mo Chen, Jinzhou Sun, and Huipeng Deng. "An Intentional Controlled Islanding Strategy Considering Island Frequency Stability for Power System with Wind Power Integrated." *Frontiers in Energy Research* 11 (2023): 1247412, https://doi.org/10.3389/fenrg.2023.1247412.

T&D World. "Southwest Power Pool Expands Service Territory into the Western Interconnection of the Nation's Power Grid." April 12, 2026. https://www.tdworld.com/utility-business/news/55370299/southwest-power-pool-expands-service-territory-into-the-western-interconnection-of-the-nations-power-grid.

Uddin, Moslem, Huadong Mo, Daoyi Dong, Sondoss Elsawah, Jianguo Zhu, and Josep M. Guerrero. "Microgrids: A Review, Outstanding Issues and Future Trends." *Energy Strategy Reviews* 49 (September 2023): 101127. https://doi.org/10.1016/j.esr.2023.101127.

US-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. April 2004. https://www.nerc.com/globalassets/our-work/reports/event-reports/august_2003_blackout_final_report.pdf.

USCC (US-China Economic and Security Review Commission). *2025 Report to Congress*. Washington, DC: USCC, November 2025. https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf.

USN (US Department of the Navy). "Groundbreaking Ceremony for Solar Facility Held at SUBASE Kings Bay." Press release, September 10, 2015. https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/2263058/groundbreaking-ceremony-for-solar-facility-held-at-subase-kings-bay/.

Vincent, Brandi. "Transportation Command Could See Expanded Contested Logistics Responsibilities Next Year." National Defense Transportation Association, August 11, 2025. https://www.ndtahq.com/transportation-command-could-see-expanded-contested-logistics-responsibilities-next-year/.

Wang, Jian-Wei, and Li-Li Rong. "Robustness of the Western United States Power Grid Under Edge Attack Strategies Due to Cascading Failures." *Safety Science* 49, no. 6 (2011): 807–812. https://doi.org/10.1016/j.ssci.2010.10.003.

Wang, Yajun, 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*. Washington, DC: IEEE, 2019. https://ieeexplore.ieee.org/document/8791601.

Winter, Jana, and Raphael Satter. "Exclusive: US Warns Hidden Radios May Be Embedded in Solar-Powered Highway Infrastructure." *Reuters*, September 10, 2025. https://www.reuters.com/legal/government/us-warns-hidden-radios-may-be-embedded-solar-powered-highway-infrastructure-2025-09-10/.

Yu, Yong, ShaoHeng Zhong, JinRong Chen, and YuBing Yang. "Selection of the Disruptive Nodes to Destroy Power Grid." In *Proceedings of the 2022 9th International Forum on Electrical Engineering and Automation (IFEEA)*. Zhuhai, China, 2022, pp. 279–282, https://ieeexplore.ieee.org/document/10037900.

Acknowledgments

My deepest appreciation goes to Steve Naumann (former vice president for transmission, Exelon), who shared strategic, operational, and technical insights that are reflected throughout this report. I would also like to thank the following colleagues for their many contributions and improvements to earlier drafts: Andy Bochman, resilience strategic lead, West Yost; Bob Butler, managing director, Cyber Strategies LLC; Jan Ithier; Miriam John, co-chair, Defense Science Board (DSB) report on Department of Defense Dependencies on Critical Infrastructure; Lance Labreck, business continuity manager, California Independent Service Operator; Mark Lauby, chief engineer, North American Electric Reliability Corporation; Judith Miller, DSB report co-chair; Richard Mroz, senior director, Archer Public Affairs; Jeffrey Price, president, Grid Options; Ryan Quint, president, Elevate Energy Consulting; Laura Schepis, vice president, government and community relations, La Plata Electric Association; Timothy Schwarz, senior manager, Emergency Management Systems Operations Support, Exelon; George D. Slessman, co-founder and CEO, DCX USA LLC; Carissa VanderMey; Bruce Walker, advisor to the associate director, Pacific Northwest National Laboratory; Mark Weatherford, head of cybersecurity policy, NVIDIA; and many current and former BPS operators who prefer to remain anonymous.

I would also like to thank my current and former colleagues at APL for their invaluable insights and editorial support: Ryan Agee, Donald P. Duncan, Timothy Frey, Kelly Livieratos, James Miller, Catherine Peacock, Erin Richardson, Matt Schaffer, Rob Schrier, Candece Seling, Paul Velez, and Ben Zintak.

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 chaired the Homeland Defense subcommittee of the Department of Defense's Reserve Forces Policy Board from 2022 to 2025. 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.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY