RESILIENCE FOR GRID SECURITY EMERGENCIES

Opportunities for Industry–Government Collaboration

National Security Perspective

Paul N. Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

RESILIENCE FOR GRID SECURITY EMERGENCIES

Opportunities for Industry–Government Collaboration

Paul N. Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Energy or any other US government agency or of JHU/APL sponsors.

NSAD-R-18-037

Contents

Figures

Figure credits:

Figure 2: "The Cyber Threat Framework," ODNI (Office of the Director of National Intelligence), n.d., https://www.dni.gov/index.php/cyber-threat-framework.

Figure 3: DHS (US Department of Homeland Security), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016).

Figure 7: Information from NERC (North American Electric Reliability Corporation), http://www.nerc.com/Pages/default.aspx; figure reprinted from Susan Lee, Michael Moskowitz, and Jane Pinelis, *Quantifying Improbability: An Analysis of the Lloyd's of London* Business Blackout *Cyber Attack Scenario*, National Security Report NSAD-R-18-027 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018).

Summary

The US Congress has opened the door to novel strategies for defending the country's electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act (FPA) in December 2015, Congress granted the secretary of energy vast new authorities to use when the president declares a grid security emergency. Most important, the secretary can issue emergency orders to power companies to protect and restore grid reliability when attacks on their systems are "imminent" or under way.[1] The FPA is silent, however, on what the secretary might require companies to do and how such orders can bolster their emergency operations.

The onset of an attack would be the worst possible time to develop emergency orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid. They could then adjust such orders to fit the specific circumstances of an attack. Developing emergency orders in advance would also help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. Companies could then exercise their contingency plans to build preparedness for response operations and contribute to national security in unprecedented ways.

This report is structured to help the electricity subsector and Department of Energy (DOE) develop emergency orders to defend the grid against potentially catastrophic cyber and physical attacks. The report highlights the phases that grid security emergencies are likely to entail. It analyzes the requirements that emergency orders will need to meet for each phase, and how orders can supplement existing utility plans and capabilities to fill gaps in grid resilience. The report also examines how emergency orders can strengthen deterrence against grid attacks and help defeat adversaries if deterrence fails.

The president must declare a grid security emergency before the secretary of energy can issue emergency orders. However, the FPA offers only broad and potentially ambiguous criteria for making that determination, especially for attacks that are imminent. Such ambiguity is useful; the president should retain the flexibility to declare grid security emergencies in a wide range of circumstances. Nevertheless, policy makers may find it useful to establish more detailed criteria to support their internal deliberations. This report proposes options for them to consider, including criteria derived from the electric industry's requirements to preserve "adequate levels of reliability" against cascading blackouts and other multistate grid disruptions. The report also examines how industry and government agencies can refine their information sharing mechanisms to support the emergency declaration process.

Once the president makes such a declaration, grid security emergencies may roll out in three phases, each of which provides the basis for developing a distinct set of template emergency orders. Figure S-1 illustrates these phases. The first will occur if the president determines that an attack is imminent. A well-established basis already exists for developing preattack emergency orders. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions. Such operations might include staffing up emergency operations centers, prepositioning recovery personnel and supplies, increasing available generation to help manage grid instabilities, and taking other precautionary measures. A key advantage of many of these options is that utilities can carry them

[1] Fixing America's Surface Transportation Act, Public Law 114-94.

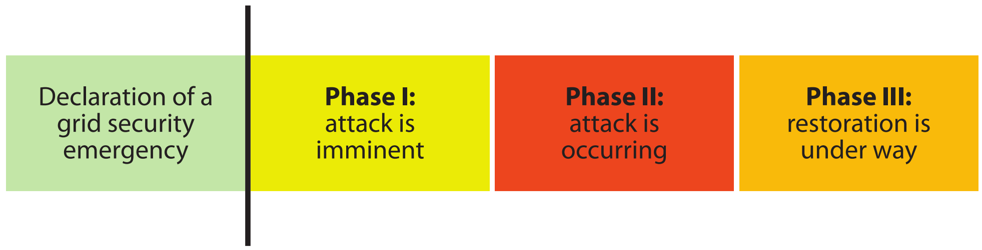

Figure S-1. Grid Security Emergency Phases

out without disrupting normal service; if the hurricane veers back to sea, utilities will have no regrets about having implemented them.

Power companies should help DOE develop equivalent "no-regrets" conservative operations to protect the grid against imminent cyber and physical attacks. A growing number of utilities are already adapting their existing plans for conservative operations to counter physical and cyber risks. These initiatives provide a strong foundation for developing emergency orders that will leverage best practices and help ensure that utilities will implement them on a consistent, nationwide basis. Moreover, because many of these conservative operations will inflict little or no disruption on normal grid service, they are ideal for protecting the grid when attacks are increasingly probable but not certain to occur. DOE and industry should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The next phase of grid security emergencies will occur when attacks are under way. Emergency orders for this phase can help utilities prevent power failures from cascading across the United States and prioritize the sustainment of electric service for military bases and facilities essential for public health (e.g., major regional hospitals and metropolitan water systems). As with conservative operations, existing electric industry plans and capabilities provide a strong basis for developing such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Orders for equivalent *extraordinary measures* could provide useful arrows in the quiver in grid security emergencies.

The final phase of grid security emergencies will commence as utilities begin restoring service to areas without power. Attacks that damage or destroy large numbers of high-voltage transformers and other difficult-to-replace grid components could create outages that darken major portions of the United States for many weeks, or even months. Power companies and DOE already have initiatives under way to meet this challenge. They should also collaborate to develop emergency orders to *support restoration*, which could facilitate the movement of replacement transformers and assist utilities in other strategically vital ways.

These grid security emergency phases could overlap. In particular, once power companies begin restoring power, adversaries may launch follow-on attacks that necessitate continued load shedding and other extraordinary measures to protect grid reliability. At the outset of an emergency, utilities should prepare to receive and implement orders across all emergency phases in an integrated way.

DOE and its industry partners should also design emergency orders to fill underlying gaps in preparedness for cyber and physical attacks. Power companies already have extensive plans and capabilities to protect and restore grid reliability against these threats, in part because mandatory reliability standards require them to do so. Grid owners and operators are also spring-loaded to employ emergency measures the moment they are needed. Indeed, the North American Reliability Corporation can fine most major US power companies if they fail to implement emergency actions to protect grid reliability.[2] This robust industry preparedness begs the question: what added value can DOE emergency orders provide?

The most obvious benefit lies in the FPA's provisions for regulatory waivers and cost recovery. When grid owners and operators carry out emergency orders, they may have to violate environmental standards and other regulatory requirements. The FPA now protects entities from being punished for such violations if they occur while complying with emergency orders. The act also provides for the recovery of costs that companies will incur in implementing emergency orders. This report examines how further waiver and cost-recovery measures could reinforce preparedness for grid security emergencies.

Emergency orders can also help support national security in new and far-reaching ways. Russia, China, and other potential adversaries will not strike the grid simply to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to US defense installations responsible for deploying forces to the region, as well as to ports and other civilian infrastructure that supports force projection. Emergency orders can be designed to help deter—and, if necessary, defeat—such attacks. This report proposes specific options to do so, in support of the *National Security Strategy of the United States of America* and other sources of US policy guidance.

Some of these options will require harsh and politically contentious decisions on allocating power if adversaries severely disrupt the grid. Emergency orders for prioritized load shedding provide a case in point. To help deter attacks, grid owners and operators need the ability to sustain service to critical defense installations, including those responsible for conducting response operations against (and imposing costs on) potential attackers for however long a conflict may last. The ability to protect power flows to hospitals and other facilities vital for public health and safety will be valuable as well. However, if adversaries disrupt sufficient grid generation and transmission assets, sustaining reliable service to these installations may require utilities to curtail service to other customers. Government officials—and, ultimately, the president—should make such decisions and provide political top cover and liability protections for power companies that implement them.

Grid security emergencies will also create unprecedented challenges for government and industry to communicate with the American people. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks. Adversaries may also disrupt the phone and internet-based communications systems utilities typically use to coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications playbooks to prepare for grid security emergencies, and they should make doing so a core component of the emergency order development process.

DOE and its industry and government partners will need to conduct intensive follow-on work to finalize the development of emergency orders and build utility-specific contingency plans to implement the orders in ways that account for accelerating structural changes in the electricity subsector. Their collaborative efforts will

[2] Bulk power system entities, including generation and high-voltage transmission companies, are subject to NERC's mandatory reliability standards and emergency orders under the FPA. For an analysis of applicability issues, see pages 5–10.

require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, as utilities and DOE tackle the immediate challenges of developing emergency orders, they should also explore broader opportunities to build preparedness for grid security emergencies. One such opportunity lies in integrating the use of emergency orders with other federal authorities. The secretary of energy can issue grid security emergency orders only to power companies. Increasingly, however, power generation depends on the flow of natural gas. Communications systems and other infrastructure sectors will also play critical roles in supporting power restoration. The secretary of energy and other federal leaders have additional authorities beyond section 215A of the FPA that can strengthen cross-sector resilience for grid security emergencies. However, achieving these benefits will require private and public sector leaders to preplan and exercise the coordinated use of these authorities, and to develop "whole-of-government" strategies to support infrastructure owners and operators.

Coordination with Canada could be valuable as well. The electric grids of the United States and Canada are deeply interconnected, and adversary-induced failures in one nation may rapidly cascade into the other. The secretary of energy does not have the authority to issue emergency orders to power companies in Canada (or in any other nation). Yet, significant opportunities exist to build on current reliability protections and emergency coordination mechanisms between US and Canadian utilities. The United States could also develop collaborative plans with Mexico as well as US allies in Europe and Asia.

In addition, DOE and its partners should explore further opportunities to help deter cyber attacks and defeat US adversaries if deterrence fails. The US *National Security Strategy* emphasizes that the United States needs to convince adversaries not only that they will suffer costly consequences if they attack but also that attacking will not accomplish the objectives they seek—in other words, achieve deterrence by denial. Yet, leading scholars of deterrence argue that deterrence by denial will be extraordinarily difficult to establish in cyberspace. Emergency orders and implementation plans can help meet these challenges by strengthening grid resilience in novel ways. Government agencies should also consider developing broader doctrine to "play defense" if cyberwarfare breaks out, and coordinate grid security emergency operations at home with measures to suppress adversary attacks at their source.

The foundational importance of the electric grid makes it a prime target for attack. As secretary of energy Richard Perry emphasizes, "America's greatness depends on a reliable, resilient electric grid" that can power the economy, support national defense, and provide for the necessities of modern life.[1] To prevent adversaries from exploiting the United States' dependence on the grid, the Department of Energy (DOE) and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter—and, if necessary, defeat—attacks on the grid.[2]

The FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the Fixing America's Surface Transportation (FAST) Act amendments to the FPA, it greatly expanded the secretary of energy's authority to issue emergency orders to grid owners and operators. Under section 215A of the act, "the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability" of critical electric infrastructure in a grid security emergency.[3] Before the secretary can issue those orders, the president must first declare a grid security emergency when attacks on the grid are imminent or under way.[4]

However, legislators provided scant guidance on what the secretary might order power companies to do. DOE and its partners in the electricity subsector are now assessing which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats. This report supports their work by examining possible emergency orders and analyzing broader opportunities to strengthen resilience for grid security emergencies.

Developing Emergency Orders under the FPA: Collaborative Opportunities, Fundamental Goals, and Overarching Design Requirements

The secretary of energy's new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, "the nine most terrifying words in the English language are 'I'm from the government and I'm here to help.' "[5] Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already taking steps to minimize such risks. Especially valuable, the department has incorporated industry recommendations on the process by which the secretary should issue emergency orders to utilities, and—"if practicable"—consult with industry before those orders are issued.[6] The next collaborative step should be to include power companies in

1 Perry, letter to the FERC.

2 The 2015 FAST Act amendments to the FPA provide the authority to undertake these efforts. Prior to 2015, section 202(c) of the FPA already authorized the secretary of energy to issue emergency orders to order "temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest." That provision also specified that the secretary could exercise such powers "during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes." See "DOE's Use of Federal Power Act Emergency Authority," DOE. The 2015 FAST Act amendments to the FPA gave the secretary further powers (mostly incorporated in section 215A of the act), which are the primary focus of this report.

3 16 U.S.C. § 824o, (b)(1).

4 The analysis that follows examines the definition of such emergencies in the FPA and potential thresholds for declaring them.

5 Reagan, "President's News Conference."

6 DOE, "RIN 1901–AB40," 1176; EEI, "Comments"; and Paradise et al., "ISO-RTO Council Comments."

designing template emergency orders. Grid owners and operators have unequaled knowledge of their own infrastructure and operating procedures and extensive experience in employing emergency measures to protect and restore grid reliability.[7] They are well positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses—and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders would be most useful to help defend their systems and effectively supplement the emergency measures utilities would already be taking on their own. Utilities will also play a critical role in building company-specific plans to implement emergency orders, exercising those plans, and identifying remaining gaps to fill.

Strategic guidance from DOE and other government departments will be just as critical for designing emergency orders. Federal leadership will be essential to ensure that emergency orders help achieve overarching US security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing emergency orders to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.[8] Government officials can also shape emergency orders and supporting initiatives to help implement US cyber resilience strategies, including the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017) and DOE's *Multiyear Plan for Energy Sector Cybersecurity* (March 2018).[9]

In addition, DOE will play critical a critical role in coordinating industry and government operations during grid security emergencies. The same congressional amendments that granted the secretary expansive new emergency authorities also specified that DOE shall be the federal government's "lead sector-specific agency for cybersecurity for the energy sector." As such, the secretary is responsible for collaborating with grid owners and operators, regulators, and other government agencies to help mitigate incidents and provide broader support to the energy sector.[10]

Federal incident response operational plans provide a broader framework for building these collaborative mechanisms. Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), the *National Cyber Incident Response Plan* (December 2016), and the *National Response Framework* (June 2016) offer particularly useful guidance for building grid-specific coordination mechanisms.[11] DOE is also strengthening its own internal mechanisms and organizational structure to manage cyber incidents.[12] These changes further position the department to effectively collaborate with industry in developing and executing emergency orders.

---

[7] FERC and NERC, *Restoration and Recovery Plans*; FERC and NERC, *Planning Restoration Absent SCADA or EMS (PRASE)*; and FERC and NERC, *Recommended Study: Blackstart Resources Availability (BRAv)*. Additional BPS plans, exercises, and mandatory reliability standards are addressed in subsequent portions of the report.

[8] White House, *National Security Strategy*.

[9] Trump, *Executive Order on Strengthening Cybersecurity*; and DOE, *Multiyear Plan*. See also Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*; and DHS, *Cybersecurity Strategy*.

[10] Fixing America's Surface Transportation Act, Public Law 114-94, 1779 (hereafter cited as FAST Act).

[11] Obama, *United States Cyber Incident Coordination*; DHS, *National Cyber Incident Response Plan*; and DHS, *National Response Framework*.

[12] DOE, *Multiyear Plan*, 28. DOE has also established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "enable more coordinated preparedness and response to natural and man-made threats." See "Secretary of Energy Forms New Office," DOE.

Drafting Template Emergency Orders before Attacks Occur

The FPA specifies that before issuing emergency orders "the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action," consult with appropriate power companies and other grid resilience stakeholders.[13] But opportunities for such consultations may be sharply limited. Adversaries may strike the grid with little or no warning. Moreover, when attacks are imminent or under way, rapidly issuing emergency orders may be crucial to help prevent cascading failures and other widespread disruptions. This imperative for speed could make consultations impractical.

To enable collaboration and minimize the risk that DOE will have to create orders amid the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, assistant secretary of energy for electricity delivery and energy reliability, stated in March 2018: "In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary's authority, while also clarifying how we communicate and coordinate the operational implementation of these orders."[14] Power companies and other electricity subsector organizations have also emphasized the need for industry and the government to jointly develop orders before adversaries strike.[15]

Such collaborative efforts should initially focus on creating *template orders*: orders that lay out the basic types of actions that the secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act amendments' potential value for the secretary to issue general orders to "protect and restore the reliability of the grid." Vague, overly broad directives cannot provide an adequate basis for utilities to develop system-specific plans to implement them. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for "maximum generation" and increased reserve margins to more aggressive, far-reaching measures.[16] A key objective for such development efforts: provide a menu of agreed-upon options from which the secretary can choose as circumstances require, supported as much as possible by consultations with industry.

Developing emergency orders before attacks occur can help ensure that, as a minimalist goal, such orders will "do no harm." By participating in the order design process, power companies can shape orders to account for system-specific engineering constraints and requirements for emergency operations. This industry input will be especially important because DOE has the authority to punish utilities for failing to comply with emergency orders, even if they are poorly designed. DOE's grid security emergency rule specifies that "in accordance with available enforcement authorities, the secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order."[17] If

[13] This includes the North American Electric Reliability Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC). 16 U.S.C. § 824o–1. See also the notice of proposed rulemaking and request for comment (DOE, "RIN 1901–AB40").

[14] Walker, *Written Testimony*.

[15] See Joint Commenters, "Comments; and NASEO, "Comments."

[16] Maximum generation involves increasing generation "above the maximum economic level" when additional generation is needed. See PJM, *PJM Manual 13*, 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help "maintain reliable operation while meeting . . . unexpected outages of existing capacity." See "M-1 Reserve Margin," NERC.

[17] DOE, "RIN 1901–AB40," 1182.

power companies find that an order is impossible to implement or is otherwise objectionable, they can ask DOE to reconsider it.[18] But adjudicating individual emergency orders amid a grid security emergency could delay time-critical actions. Instead, DOE should include industry in developing emergency orders from the start and resolve utility concerns before adversaries strike.

Preplanning to coordinate industry and government emergency operations will also be valuable. Power companies are already poised to take immediate emergency actions to protect grid reliability as circumstances require, regardless of whether the secretary issues emergency orders. It will be helpful to understand in advance how DOE can best align the issuance of such orders with industry-initiated actions. Once attacks are under way, preplanning for operational coordination will become still more important, especially if adversaries continue striking the grid and its supporting communications systems after their initial salvo.

If attacks do occur, Russia, China, or other potential adversaries will use country-specific tactics, techniques, and procedures to disrupt US infrastructure. Defending against those attacks will require tactical and operational responses that are similarly tailored to specific adversaries. Over time, it may be possible to develop (and protect adversaries from accessing) emergency orders that account for these individualized defensive requirements. US leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this report examines opportunities to do so.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high-voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military bases, regional hospitals, and other critical customers that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and identify opportunities to improve order design and execution. Training programs to prepare employees to carry out utility-specific implementation plans should also get under way as soon as possible. On a larger scale, utilities will also be able to exercise the implementation of template emergency orders within the framework of the Cyber Mutual Assistance (CMA) Program. This program enables over 140 utilities in the United States and Canada to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.[19] Exercises can help determine how best to align the issuance and implementation of emergency orders with these growing capabilities for mutual support.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the secretary of energy has the sole authority to issue emergency orders, the secretary may request input from senior DOE staffers

[18] DOE, "RIN 1901–AB40," 1181–1182.

[19] "ESCC's Cyber Mutual Assistance Program," ESCC.

on which orders will be most useful against specific types of attacks. The secretary may also need to brief the president and the National Security Council on proposed orders and their potential benefits. By developing orders and clarifying their respective advantages before adversaries strike, DOE and industry partners can facilitate such deliberations.

Over the longer term, industry and government leaders might structure their collaboration to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public–private and interagency coordination.[20] Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government–industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, to develop template emergency orders and contingency plans to implement them, power companies will need to conduct extensive operational and engineering studies and use enhanced modeling to understand the potential impact of such orders. The FAST Act amendments to the FPA provide no funding for such development efforts. Moreover, DOE and power companies are only the most obvious participants in the order design process. A wide array of other grid resilience and incident management stakeholders may also need to assist that process—including critical ones not mentioned in the FPA. Determining which specific public and private sector organizations should help shape template orders constitutes a critical first step in preparing for grid security emergencies.

[20] Danzig, *Catastrophic Bioterrorism*, 5–7; and Blue Ribbon Study Panel, *National Blueprint*, 13, 42–44.

Participants in Drafting and Implementing Emergency Orders: The Bulk Power System and the Broader Electricity Subsector

An initial task in developing emergency orders will be to determine which components of the electricity subsector should participate in that effort. DOE defines the electricity subsector as the "portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity."[21] The most obvious candidates for inclusion are the power companies that are subject to emergency orders. The FAST Act amendments to the FPA specify which components fall into that category. Chief among them are "any owner, use or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States."[22] The FPA also includes criteria to identify this infrastructure. Critical electric infrastructure comprises grid systems or assets whose incapacity or destruction would "negatively affect national security, economic security, public health and safety, or any combination of such matters."[23] Defense critical electric infrastructure consists of grid components that serve facilities "critical to the defense of the United States" and that are vulnerable to the disruption of grid-provided power.[24]

However, Congress also narrowed the definition of critical electric infrastructure in a significant way. The FPA states that such infrastructure only includes assets that compose the bulk power system (BPS). BPS assets are those "facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation

[21] DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

[22] 16 U.S.C. § 824o–1, (b)(4)(c).

[23] 16 U.S.C. § 824o–1, (a)(2).

[24] 16 U.S.C. § 824o–1, (a)(4).

facilities needed to maintain transmission system reliability."[25] These BPS generation and transmission assets provide synchronized power within the three interconnections that serve the entire United States and parts of Mexico and Canada.[26]

As defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.[27] That limitation creates a potential problem for executing emergency orders. Local distribution systems often provide the "last mile" of connectivity between transmission systems and military bases and other critical customers. As DOE and industry create template emergency orders and execution plans, it will be essential to integrate local distribution providers into that development process.

However, before examining these distribution-level issues, it will first be helpful to clarify the components of the BPS that are explicitly subject to emergency orders under the FPA (and are therefore key partners for DOE in designing them). The FPA states that the secretary of energy may issue emergency orders to the following the BPS "entities:" [28]

The Electric Reliability Organization. After blackouts cascaded across major portions of the United States in August 2003, Congress authorized the Federal Energy Regulatory Commission (FERC) to certify an electric reliability organization to develop and enforce, subject to FERC approval, mandatory electric reliability standards for all users, owners, and operators of the US BPS.[29] FERC certified the North American Electric Reliability Council (NERC) as the first-ever electric reliability organization in July 2006. Renamed the North American Electric Reliability Corporation in 2007, it has served in that role since.[30] NERC's mission is to ensure the reliability and security of the BPS in North America. As such, NERC is uniquely positioned to help DOE develop emergency orders, especially for attacks that could create cascading blackouts or other multistate disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a leading role for the electricity subsector in establishing situational awareness, incident management and coordination, and communication capabilities.[31] E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be vital for responding to grid security emergencies.

Regional entities responsible for enforcing reliability standards for the BPS.[32] NERC has delegated certain authorities to eight regional entities to monitor and enforce compliance with reliability standards.[33] While regional entities play major oversight roles, they do not directly operate the physical grid and would not, on their own, be positioned to execute emergency orders. However, they could help utilities and DOE and preplan for

25 16 U.S.C. § 824o, (a)(1).

26 Interconnections are defined as the "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." North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See NERC, *Glossary*.

27 The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify "local" distribution. See 16 U.S.C. § 824o, (a).

28 16 U.S.C. § 824o–1, (b)(4).

29 Energy Policy Act of 2005, Public Law 109-58. This does not include Alaska or Hawaii.

30 NERC, *History*. For more information on NERC, see "About NERC," NERC.

31 "Electricity Information Sharing and Analysis Center," NERC.

32 DOE, "RIN 1901–AB40," 1177. See also 16 U.S.C. § 824o, (a)(7).

33 "Key Players," NERC. In July 2017, however, one regional entity announced its intention to dissolve. FERC has approved the dissolution, effective July 2018. See FERC, *Order Granting Approvals* (163 FERC ¶ 61,094).

issuing regulatory waivers to BPS grid operators as they comply with emergency orders.

Owners, users, and operators of critical electric infrastructure or defense critical electric infrastructure within the United States.[34] Companies that own and operate generation and transmission assets will be among the most likely recipients of emergency orders and should play a critical role in designing them. Reliability coordinators will be similarly important. Reliability coordinators are the entities that constitute "the highest level of authority" for the reliable operation of the bulk electric system (BES).[35] They are also responsible for maintaining a "wide-area view" of the BES and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, reliability coordinators will be critical for designing, receiving, and implementing emergency orders to counter attacks that individual BPS owners and operators may not have the ability to defeat. Seven regional transmission organizations and independent system operators, most of which are registered as reliability coordinators, also help operate and ensure the reliability of the BES in many regions of the United States.[36] Accordingly, regional transmission organizations and independent system operators will be essential to the design and execution of emergency orders.

Local Distribution Providers and Other Grid Resilience Stakeholders

The 2015 FAST Act amendments to the FPA do not explicitly address the possible roles of local distribution systems in grid security emergencies. However, local distribution infrastructure is critical for overall resilience against cyber and physical attacks. Even if emergency orders help defeat attacks on BPS assets, adversaries may still be able to achieve catastrophic effects by striking multiple local distribution systems and thereby interrupting the flow of power from transmission systems to military bases, hospitals, and other end users. Local distribution systems may also need to help implement emergency orders issued to BPS entities. For example, if the secretary orders transmission systems to protect reliability by shedding load, yet at the same time sustain the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding. Holistic preparedness for grid security emergencies therefore requires engagement with local distribution systems.

These systems will also have strong incentives to participate in the emergency order planning process. Just as BPS entities rely on local distribution utilities, these utilities rely on generation, transmission, and higher-voltage distribution entities to serve end users. Local systems will also share the commitment of BPS entities to protect and rapidly restore service to defense installations and other critical customers. By integrating local distribution utilities

---

[34] The analysis that follows later in this section examines the definition of "users" of critical electric infrastructure and defense critical electric infrastructure.

[35] While the BPS broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the BES is a subset of the BPS that includes, with some exclusions, all transmission and real and reactive power sources at one hundred kilovolts or higher. As with the BPS definition, the BES definition excludes local distribution providers. For these definitions, as well as the definition of reliability coordinators, see NERC, *Glossary*. Consistent with the FPA and the authorities it provides for handling grid security emergencies, this report focuses on the application of emergency orders to BPS entities specifically.

[36] There are ten regional transmission organizations and independent system operators under NERC's purview, though three operate exclusively in Canada. Regional transmission organizations and independent system operators are independent membership-based nonprofit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are operated by individual utilities or utility holding companies. See "About 60% of U.S. Electric Power Supply Managed by RTOs," US Energy Information Administration. Six of the seven regional transmission organizations/independent system operators operating in the US are also current reliability coordinators. See "Reliability Coordinators," NERC.

into emergency order planning, these utilities will be able to participate in shaping template orders and implementation plans to help achieve their reliability goals when adversaries strike. Moreover, to the extent that local distribution companies may be subject to emergency orders, they may also benefit from the FPA's liability protections and cost-recovery provisions for actions taken to execute those orders.

DOE and other stakeholders may determine that the FPA already gives the secretary adequate authority to issue emergency orders to local distribution companies. The act states that emergency orders may apply to "any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure" within the United States.[37] The act, however, does not further define owners, users, and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the act.

Regardless of whether the secretary can issue orders to local distribution utilities, BPS entities should include them in building the contingency plans to implement emergency orders. This preplanning will be essential to strengthen comprehensive, end-to-end protection of grid reliability against attacks.

Many companies that own transmission assets also own distribution infrastructure. These utilities will find it relatively easy to include distribution assets in their emergency planning. Integrated response plans will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for "vertically integrated" utilities that own and operate assets for all three functions. However, many municipally owned electric utilities and rural electric cooperatives (including those that serve critical and defense critical electric infrastructure) are not part of vertically integrated companies. In US regions where generation, transmission, and distribution systems exist as separate entities, additional engagement initiatives will be essential to implement emergency orders and sustain power to essential facilities.

Including state regulators and other state officials in these integrative efforts could offer additional benefits. State public utility commissions have primary regulatory jurisdiction over distribution systems.[38] The National Association of Regulatory Utility Commissioners, which represents state regulators nationwide, has focused growing attention on the need for prudent utility investments in cyber and physical resilience.[39] Commissioners in New Jersey and other states are also leading regulatory initiatives to bolster cyber resilience in their respective jurisdictions.[40] Emergency managers and National Guard leaders in a growing number of states are also building new mechanisms to coordinate with utilities in responding to cyber attacks. Adding such additional partners to help design emergency orders and plan for their implementation would complicate an already far-reaching engagement process. Nevertheless, incorporating perspectives from state commissioners and other officials would help advance comprehensive state-level preparedness for grid security emergencies.

Additional Partners for Engagement

DOE and power companies will need to collaborate with a wider array of partners to develop and execute some potentially useful emergency orders, especially to support grid restoration. The final rule

37 16 U.S.C. § 824o, (b)(4)(a).

38 The US Constitution, in most cases, allows federal regulation of private economic activity only for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See Lazar, *Electricity Regulation in the US*, 15.

39 See NARUC, *Cybersecurity*; and NARUC, *Resolution on Physical Security.*

40 State of New Jersey Board of Public Utilities, *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196).

on *Grid Security Emergency Orders: Procedures for Issuance* (hereinafter referred to as the grid security emergency rule) notes: "Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits" to expedite the restoration of power.[41] This includes traditional partners such as the Department of Homeland Security (DHS) and the Department of Defense (DOD). Still broader collaboration with government and private sector partners may be valuable for implementing emergency orders to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy large power transformers at substations across the United States, and these attacks cut off power to critical military bases, the secretary might order industry to prioritize the replacement of large power transformers at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program to provide for such replacements.[42] New industry-led organizations such as Grid Assurance,[43] as well as programs such as the Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) initiative, are further expanding the industry's capacity to replace transformers and other equipment.[44] These efforts will be essential for preparing for grid security emergencies, especially as industry stocks and securely stores the full range of replacement transformer types and sizes that large-scale physical attacks may require.

However, power companies do not move large power transformers by themselves. They rely on railroad companies, barges, and heavy-haul trucking companies to help do so and have established a Transformer Transportation Working Group under the ESCC to plan and coordinate transformer movement.[45] Exercises in the Spare Transformer Equipment Program now involve representation from transportation stakeholders. Yet, the FPA does not give the secretary authority to issue orders to transportation companies. In anticipation of orders for replacing transformers, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Preplanning with the US Department of Transportation (DOT), the Federal Emergency Management Agency (FEMA), and state governments to get contracts, permits, and regulatory waivers to expedite transformer movement will also be useful. In addition, advance coordination with emergency managers at all levels of government would help them mitigate the effects of rotating blackouts or other extraordinary measures on public health and safety.

DOE and the electricity subsector should consider expanding the geographic scope of these discussions as well. In defining the defense critical electric infrastructure that emergency orders can protect, Congress excluded grid assets in Alaska and Hawaii.[46] But both states are home to vital military installations, as are a number of US territories. The secretary also lacks the authority to issue emergency orders to Canadian utilities. Yet, US and Canadian electric systems are deeply integrated, and coordinated efforts to prevent instabilities in grid security emergencies could benefit both nations. Collaborations with NATO allies and other security partners in the face of major adversarial cyber campaigns could be valuable as well. The concluding section of this report examines the potential benefits of expanding grid

41 DOE, "RIN 1901–AB40," 1177.

42 See DOE, *Strategic Transformer Reserve*; and "Spare Transformers," EEI.

43 "Transmission Equipment Ready," Grid Assurance.

44 FERC, *Order Authorizing Acquisition and Disposition* (163 FERC ¶ 61,005), 10.

45 DOE, *Strategic Transformer Reserve*, 12.

46 16 U.S.C. § 824o–1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

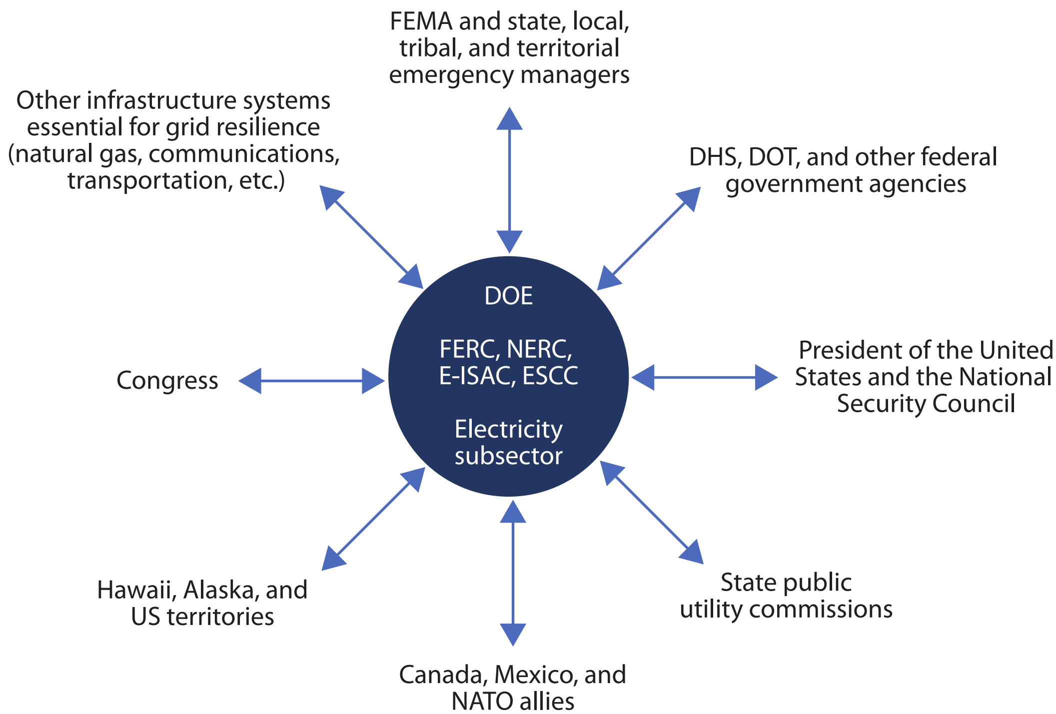

Figure 1. Stakeholders for Building Grid Security Emergency Resilience

security emergency coordination within the United States and beyond.

Figure 1 illustrates the array of partners that might help build preparedness for such emergencies. DOE, BPS entities, and the broader electricity subsector comprise the core of the team needed to design, issue, and implement emergency orders. DOE defines the electricity subsector as the "portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity."[47] This definition comprises the key subsector components represented in the ESCC, to include owners and operators of electric generation, transmission, and distribution assets "from all ownership categories."[48] As such, the ESCC is ideally suited to coordinate with DOE in the order development process, together with NERC, the E-ISAC, and other BPS entities and trade associations.

Surrounding these core participants are additional partners that might offer valuable insights for developing orders and coordinating emergency response operations. Some of these partners (including Congress) can also help oversee the implementation of the FPA's emergency provisions and assess requirements for further statutory changes.

Of course, the full set of potential contributors to emergency preparedness is broader still. For example, vendors who can help utilities replace damaged relays and other equipment could play vital roles. So could law enforcement agencies, cybersecurity contractors, state National Guard organizations, and other sources of expertise and support for power companies. National laboratories and other research and development organizations will also need to sustain their support for improved grid resilience. Over time, comprehensive engagement with all such partners could pay major dividends.

[47] DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

[48] In addition to infrastructure owners and operators, ESCC membership includes regional transmission organizations and independent system operators, NERC, the National Infrastructure Advisory Council, and the Canadian Electricity Association. ESCC, *Electricity Sub-Sector Coordinating Council Charter*, 3.

Goals and Specific Design Requirements for Developing Emergency Orders

The starting point in developing template emergency orders is to identify the objectives, scope, and design requirements that these orders will need to encompass. Key issues analyzed in the sections of the report that follow:

- **Threats, triggers, and thresholds for issuing emergency orders.** Only a limited number of natural and man-made hazards can trigger a grid security emergency.[49] Countering each of those hazards will require threat-specific emergency orders. Hence, the first step for developing such orders will be to examine the threats and attack scenarios on which the design process should focus and clarify the criteria that the president might use to determine that a grid security emergency exists—including when there is an "imminent danger" of an attack.

- **Designing emergency orders for sequential phases of grid security emergencies.** Different types of emergency orders will be needed to protect grid reliability (1) when attacks are imminent, and (2) when attacks are under way. Promising opportunities also exist to develop orders for a third phase of grid security emergency operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.

- **Incorporating national security policies and priorities into emergency order design.** Adversaries may strike the grid to disrupt the flow of power to defense installations and other facilities essential to national security. Many utilities are already collaborating with defense partners to build redundant power feeds for these facilities and make other targeted investments in resilience. A growing number of grid owners and operators also plan to prioritize the restoration of power to military bases if blackouts occur. Emergency orders provide a unique opportunity for DOE and its partners to build on such initiatives, and provide more systematic, comprehensive, and effective support to national security.

An initial step to do so is to ensure that emergency orders reflect and help achieve broader federal government strategies to defend critical infrastructure. Most important, the US *National Security Strategy* specifies how the United States will deter attacks on critical systems and—if deterrence fails—how it will defeat the attackers.[50] DOE and its industry partners should design emergency orders to help implement the strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this design process with two further steps. First, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. The FPA provisions and existing industry plans to prioritize the restoration of power will provide a useful starting point. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement emergency orders and help defend the nation.

Emergency orders and implementation plans also offer a basis to clarify how US agencies and private companies will coordinate their operations during cyberwarfare, and build consensus on the private sector's emerging role in national security. No power company has ever tried to maximize shareholder value by promising to bolster cyber deterrence or help defeat attacks by nations such as Russia or China. Yet, because

[49] In addition to being triggered by cyber attacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, (a)(7).

[50] White House, *National Security Strategy*, 13.

of the grid's importance to the economy, public health and safety, and national defense, the United States needs a doctrinal framework to coordinate industry and government actions during attacks on the US electric system.[51] Scott Aaronson, Edison Electric Institute's vice president for security and preparedness, notes that "there is not a lot of doctrine around cyber attacks on civilian infrastructure."[52] Building such doctrine and operationalizing public–private partnerships will be crucial for grid security emergency preparedness.

- **Communications.** The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The grid security emergency rule describes the consultative process that (if practicable) will occur before the secretary issues emergency orders.[53] However, the grid security emergency rule does not address the risk that adversaries will attack the industry–government communications systems necessary to issue orders, monitor their implementation, and defeat adversaries' attacks.

  Building secure, survivable communications will be essential to effectively issuing and implementing emergency orders. However, the FPA provides no requirements or funding to do so. The electricity subsector is currently working with government agencies and telecommunications companies to advance secure communications initiatives. These partners should treat preparedness for grid security emergencies as a special area of focus, including measures to ensure that grid owners and operators can verify the authenticity of emergency orders.

  Government and utility leaders will also need to coordinate what they tell the American people when the secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including those for prioritized load shedding, could cut off electricity to many thousands of customers. Emergency orders that will have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

  Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Attackers will strike the grid to achieve political benefits, including, potentially, the incitement of public panic and a loss of confidence in US leaders. To promote unity of messaging against such efforts, it will be essential to build on existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders.

- **Waivers and cost recovery.** Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the act itself, FERC-approved reliability standards, or environmental regulations.[54] However, emergency orders will be easier to implement if they include preplanned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

[51] For DOD's definition of doctrine and an analysis of its benefits for joint warfighting, see Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United State*.

[52] Lynch, "How the Russian Government Allegedly Attacks."

[53] DOE, "RIN 1901–AB40," 1181.

[54] These waivers apply unless companies carry out orders and related actions in a "grossly negligent manner." See 16 U.S.C. § 824o–1, (f)(4).

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.[55] Industry–government dialogue will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader preplanning needed for the financial turbulence that grid security emergencies could create. This study also examines possible emergency orders that would require investments in grid infrastructure to implement. The FPA does not authorize government spending on such pre-emergency projects. If DOE and its partners decide that investment-dependent orders have sufficient value for grid resilience, these partners (and Congress) should explore government funding options that reflect the national security benefits of such orders, rather than increase the electricity bills paid by private citizens.

- **Opportunities for broader resilience against grid security emergencies.** Power companies and DOE may find it helpful to develop a comprehensive plan to sequence and integrate all of the initiatives outlined above. Such a plan might also account for three additional opportunities for progress: (1) employing additional government authorities to coordinate emergency operations between electric utilities and companies in other infrastructure sectors, including the natural gas providers on which power generation increasingly depends; (2) deepening US partnerships with Canada to help protect the interconnected North American power grid, and exploring opportunities for collaboration with Mexico and other nations; and (3) examining longer-term opportunities to leverage improvements in grid resilience to strengthen cyber deterrence, and assessing the risks and potential benefits of coordinating cyber defense operations at home and abroad.

[55] 16 U.S.C. § 824o–1, (b)(6).

Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies

The FPA leaves the president substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should build consensus on the types of threats that ought to drive and sequence the development process. These partners should also examine possible decision criteria and consultative mechanisms to support declarations of grid security emergencies.

Threats That Can Trigger Grid Security Emergencies: Implications for Emergency Order Design

A broad array of natural and man-made hazards, including earthquakes and severe weather events such as hurricanes and ice storms, can cause multistate blackouts. However, in amending the FPA, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the "occurrence or imminent danger" of:

> (A)
>
> (i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;[56] and
>
> (ii) disruption of the operation of such devices or networks, with significant adverse

[56] The second section of this report defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of grid security emergency thresholds.

effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event; or

(B)

(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.[57]

Protecting critical and defense critical electric infrastructure against each of these threats will require different types of emergency orders—though some potential orders may be useful against multiple hazards. The threats will also pose disparate challenges for determining whether a grid security emergency is imminent or under way. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the president faces uncertainties about the likelihood and potential consequences of a grid security emergency.

Geomagnetic Storms as a Possible Initial Focus

Emergency orders for geomagnetic disturbances will entail fewer design challenges than those for cyber attacks and other man-made hazards, and therefore provide opportunities for rapid progress. Geomagnetic disturbance events occur when coronal mass ejections on the sun create geomagnetically induced currents on the earth's surface. These currents can damage unprotected transformers and other grid infrastructure. Compared with the other threats that can trigger grid security emergencies, determining that there is imminent danger of a geomagnetic disturbance event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the president decide whether to declare a grid security emergency and will provide significant warning before geomagnetically induced currents threaten to damage grid infrastructure.

Industry and government partners can develop emergency orders to take advantage of this warning time. For example, the secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of geomagnetically induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.[58]

A strong foundation already exists for drafting such orders. Studies of the effects of geomagnetic disturbances on the power grid have contributed to a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.[59] Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the federal government to ensure that it has the capability to predict and detect space weather events and the ability to communicate these assessments to public and private sector stakeholders. The order also requires the development of protection and mitigation plans for critical infrastructure and plans for response and recovery if geomagnetic disturbances occur. In addition, the order requires sector-specific agencies to "assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event."[60]

NERC reliability standards provide an additional cornerstone for developing emergency orders for geomagnetic disturbances. TPL-007-1—*Transmission System Planned Performance for Geomagnetic*

57 16 U.S.C. § 824o–1, (a)(7).

58 Phillips, "Solar Shield." See also MISO, *Geomagnetic Disturbance Operations Plan*, 5.

59 See "NOAA Space Weather Scales," NOAA; and Kappenman, *Geomagnetic Storms*.

60 Obama, *Executive Order—Coordinating Efforts*.

Disturbance Events establishes long-lead geomagnetic disturbance planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat for geomagnetic disturbance events.[61] EOP-010-1—*Geomagnetic Disturbance Operations* also requires reliability coordinators to develop geomagnetic disturbance mitigation plans and operating procedures, including specific actions that transmission operators must take based on predetermined geomagnetic disturbance-related conditions.[62]

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyber attacks and other man-made triggers for grid security emergencies. The sun will not intentionally hide preparations for a geomagnetic disturbance event or "prepare the battlefield" by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data that utility personnel need to maintain situational awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of critical and defense critical electric infrastructure.

The relative ease of drafting orders for geomagnetic disturbances makes such efforts a prime starting point for industry–government collaboration. The North American Transmission Forum, in coordination with the ESCC, is already examining opportunities to develop template emergency orders for geomagnetic disturbance events. But the greater degree of difficulty associated with protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of emergency orders to counter such threats. Instead, DOE and its industry partners should consider pursuing a multitrack development process: at the same time that they seek rapid progress on emergency orders for geomagnetic disturbances, they should *immediately* accelerate the long-lead work that will be required to counter each of the man-made threats that can trigger grid security emergencies.

Cyber and Physical Attacks

This report focuses on supporting the development of emergency orders to protect and restore grid reliability against cyber and physical attacks. In doing so, the report follows the lead of the premier electric industry exercise of grid resilience, GridEx. As in previous versions of this exercise series, GridEx IV (conducted in November 2017) employed a scenario based on large-scale, combined cyber and physical attacks against the US electric system by a highly capable adversary.[63] Such combined attacks could pose severe threats to nationwide grid reliability, over and above those created by cyber or physical strikes alone. Grid security emergency orders that can help power companies protect and restore reliability against combined attacks will be especially valuable for national security. Orders and implementation plans that can help counter such severe threats will also be useful in lesser contingencies, including cyber-only strikes.

Current US policy priorities focus on the need to strengthen cyber resilience for the power grid and other critical infrastructure. The US *National Security Strategy* warns that cyber weapons "enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces."[64] DOE and its partner utilities should prioritize the development of emergency

[61] NERC, *TPL-007-1*.

[62] The standard, however, does not explicitly lay out what those predetermined conditions should be. See NERC, *EOP-010-1*. For an example of geomagnetic disturbance plans, see PJM, *PJM Manual 13*, 69–71.

[63] GridEx includes participation by over one hundred power companies and other components of the electricity subsector. See NERC, *Grid Security Exercise GridEx IV*, vii.

[64] White House, *National Security Strategy*, 12, 27.

orders to counter such attacks, and supplement the mandatory and increasingly stringent cyber critical infrastructure protection standards, as well as voluntary measures that go above and beyond those NERC requirements.[65]

However, orders can also help build resilience against physical attacks on the grid. Since the coordinated attack on the Metcalf substation near San Jose, California, in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high-powered rifles or other weapons. This includes NERC's *CIP-014-2—Physical Security* standard, which outlines the requirements for protecting grid infrastructure from physical attacks.[66] Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

An adversary would face greater risks when launching physical attacks than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger-scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk–reward calculus in our favor. If orders can help power companies protect their systems from impending physical attacks, especially in partnership with state and local law enforcement agencies, state National Guard personnel, and other sources of assistance, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Adversaries may also simultaneously employ both cyber and physical attacks. Such combined attacks can synergistically disrupt the grid in ways that cyber or physical attacks on their own cannot. For example, as in the response to cyber attacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.[67] However, physical attacks that destroy critical substation components or target utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

The GridEx IV scenario highlighted the unique challenges posed by combined attacks and opportunities to address them. That scenario also assumed that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past US power outage.

This report adopts a similarly severe threat for analyzing possible emergency orders. In particular, the report examines how orders can protect or restore grid reliability against the combined use of cyber weapons, physical attacks, and information

[65] NERC has mandatory standards for critical infrastructure protection against cyber threats. See "United States Mandatory Standards," NERC.

[66] DOE, *Quadrennial Energy Review*, 4–34; and NERC, *CIP-014-2*.

[67] E-ISAC and SANS-ICS, *Analysis of Cyber Attack*, v.

warfare against critical and defense critical electric infrastructure. Of course, separate types of emergency orders will be required for physical and cyber threats. Orders to deploy specific countermeasures against unmanned aerial vehicle attacks on substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead, utilities can also benefit from examining how emergency orders could help them defeat combined attacks, and how they can integrate both cyber and physical defense operations.

The study does not examine options for developing emergency orders against electromagnetic pulse (EMP) attacks. EMP threats pose a significant potential risk to the grid, and a growing (though still relatively small) number of utilities are hardening their critical systems against EMP effects.[68] DOE's EMP strategy provides a valuable framework and approach for managing the risks that EMP threats pose to the grid and other energy systems.[69] DHS's EMP strategy does the same for a broad range of infrastructure sectors.[70] Industry partners such as the Electric Power Research Institute are also making notable contributions to the shared understanding of EMP effects on the grid.[71] However, significant research is still required to understand the combined effects of EMP wave components on grid hardware and system-wide operations and for cost-effective mitigation options and preparedness planning.[72] As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

Thresholds for Declaring Grid Security Emergencies[73]

The FPA authorizes the president to declare a grid security emergency when there is "imminent danger" of an attack or when attacks are already occurring. However, the FPA does not further define imminent, nor provide any criteria to help determine whether the anticipated likelihood of an attack is sufficient to warrant an emergency declaration. As will be discussed below, the FPA provides guidance on the potential severity of imminent or ongoing attacks that would constitute a grid security emergency. However, those guidelines are broad and could be subject to starkly different interpretations in future crises.

Some degree of ambiguity is useful. Preserving wide presidential latitude for declaring grid security emergencies will be essential to deal with unforeseen challenges and to avoid locking US crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger a declaration. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay US defensive measures, including the issuance of emergency orders to safeguard the grid. Adversaries might even seek to spoof the president into declaring a grid security emergency when they had no intention of launching an attack—especially if adversaries believed doing so might prompt the issuance of disruptive emergency orders, crash utility stock

68 In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to geomagnetic disturbances. The early-time component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See EPRI, *Electromagnetic Pulse and Intentional EMI Threats*, 3-3–3-4.

69 DOE set strategic goals for addressing EMP threats and created an action plan to meet those goals. DOE, *Electromagnetic Pulse Resilience Action Plan*. The fiscal year 2017 National Defense Authorization Act directed DHS to create a similar strategy, which is currently in draft form. See National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328. The EPRI continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse*.

70 DHS, *Strategy for Protecting and Preparing*.

71 EPRI, *Electromagnetic Pulse and Intentional EMI Threats*.

72 INL, *Strategies, Protections, and Mitigations*.

73 The analysis in this section builds on the findings of Stockton, "Thresholds."

prices, or incite public panic in ways that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events that emergency orders should be designed to help counter.[74] Federal officials could also find it useful to have decision criteria to help frame their own internal deliberations and recommendations to the president. In an intense crisis, ambiguities in the FPA could fuel disagreements among the president's advisors as to whether the threat of attack was sufficiently severe to declare a grid security emergency. Developing a decision framework to support the declaration process could facilitate consensus-building and provide a structured way to integrate data on attack indicators. However, in adopting such a framework, it would also be prudent to avoid revealing any specific declaration triggers or thresholds for adversaries to exploit in their attack planning.

The section that follows examines two factors that a decision framework might encompass: the likelihood of an attack occurring and its potential consequences. This section also examines how improved information sharing between government agencies and power companies can support these assessments and recommends industry–government consultations in the declaration process that go beyond the existing provisions of the FPA.

Determining When Attacks Are Imminent: Criteria for Declaring Grid Security Emergencies

In key respects, the BPS is under cyber attack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS networks, secrete malware designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.[75] PJM Interconnection's former CEO Terry Boston recently stated that the company experiences three thousand to four thousand hacking attempts *every month*.[76] Penetration efforts on a similarly massive scale are likely occurring against BPS entities across the United States. While many of these efforts target information technology systems not directly involved in operating the grid, malware implants on operational technology systems are increasingly frequent and sophisticated.[77] And, as in the case of BlackEnergy and other campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.[78] The net result, according to US director of national intelligence Dan Coats: "Today, the digital infrastructure that serves this country is literally under attack."[79]

Of course, there is a huge gulf between implanting destructive malware on the grid and using that malware to create blackouts. The Trump administration has promised to impose "swift and costly consequences" on foreign governments and other actors who undertake "significant malicious cyber activities" against US critical infrastructure.[80] Attacks that create massive power outages and jeopardize US national security would be especially likely to provoke such a response. However, the president does not need to wait for blackouts to occur before declaring

74 Paradise et al., "ISO-RTO Council Comments," 2.

75 "Alert (TA18-074A)"; "Alert (TA17-293A)"; Defense Science Board, *Task Force on Cyber Deterrence*, 4; and ICF International, *Electric Grid Security and Resilience*, 19.

76 Dougherty, "Biggest U.S. Power Grid Operator Suffers Attacks."

77 "Alert (TA17-293A)"; and "Alert (TA18-074A)."

78 BlackEnergy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of BlackEnergy inflicted the 2016 blackout on Ukraine. "Alert (ICS-ALERT-14-281-01E)."

79 Barnes, "Warning Lights."

80 White House, *National Security Strategy*, 13.

a grid security emergency. The "imminent danger" of attack is sufficient to declare an emergency and for the secretary to issue orders to help utilities ramp up their defenses.

Implants of new, potentially devastating malware across the electric grid could help the president make such a determination, particularly if other warning indicators suggest that cyber attacks are becoming increasingly likely. The geopolitical context in which cyber attacks might occur provides one such indicator. It is (barely) conceivable that adversaries will launch a "bolt from the blue" attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region and attack the grid to disrupt the deployment of US forces to the region or to achieve other military and political goals.[81] Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause multistate blackouts, should carry greater weight in a crisis environment.

Policy makers should consider developing a framework to assess whether these cyber preparations help justify the declaration of a grid security emergency. The US Office of the Director of National Intelligence (ODNI) has issued a cyber threat framework that could support such development efforts. The ODNI notes that government agencies, academia, and the private sector are using over a dozen analytic models to categorize cyber threats and identify changes in the activities of cyber adversaries. ODNI's framework is intended to provide a common basis for characterizing threat activity to support analysis and senior-level decision-making.[82] Figure 2 illustrates the cyber threat framework.

[81] The section on preattack grid security emergency declarations examines these national security–related issues and their implications for designing emergency orders.

[82] "Cyber Threat Framework," ODNI; and ODNI, *Common Threat Framework*, 5.

The initial stage of adversary activity is to prepare for conducting malicious activity. Adversaries then engage and establish presence on targeted systems, allowing them to "operate at will." In the final stages, attackers seek to destroy grid hardware, software, and/or data, and prepare to conduct follow-on operations as needed to magnify the extent and duration of their disruptive effects.[83]

If adversaries were to suddenly make new moves into the penultimate phase (operate at will) during an intense political crisis or regional confrontation, evidence that they had done so could help the president determine whether attacks were imminent. Other independent sources of data could provide additional context for assessing adversary moves toward more threatening preattack stages. James Miller, former undersecretary of defense for policy, notes that "the United States devotes massive resources to human and technical intelligence collection of our potential adversaries."[84] Such indicators could contribute to overall assessments of attack imminence.

Policy makers might also supplement the cyber threat framework with specialized attack models for the industrial control systems and other grid components that are crucial for electric system operations. The Industrial Control System Cyber Kill Chain provides an especially promising opportunity to do so. The kill chain identifies the specific sequenced phases that adversaries execute to conduct attacks that inflict predictable physical effects on grid equipment and operations.[85] Stage 1 begins with planning and reconnaissance against

[83] ODNI, *Common Threat Framework*, 13, 16.

[84] Miller, "Cyber Deterrence."

[85] The Industrial Control System Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 to "help the decision-making process for better detecting and responding to adversary intrusions." The Industrial Control System Cyber Kill Chain tailors that decision-making tool for industrial control system–specific cyber threats and consequences. See Assante and Lee, *Industrial Control System Cyber Kill Chain*.

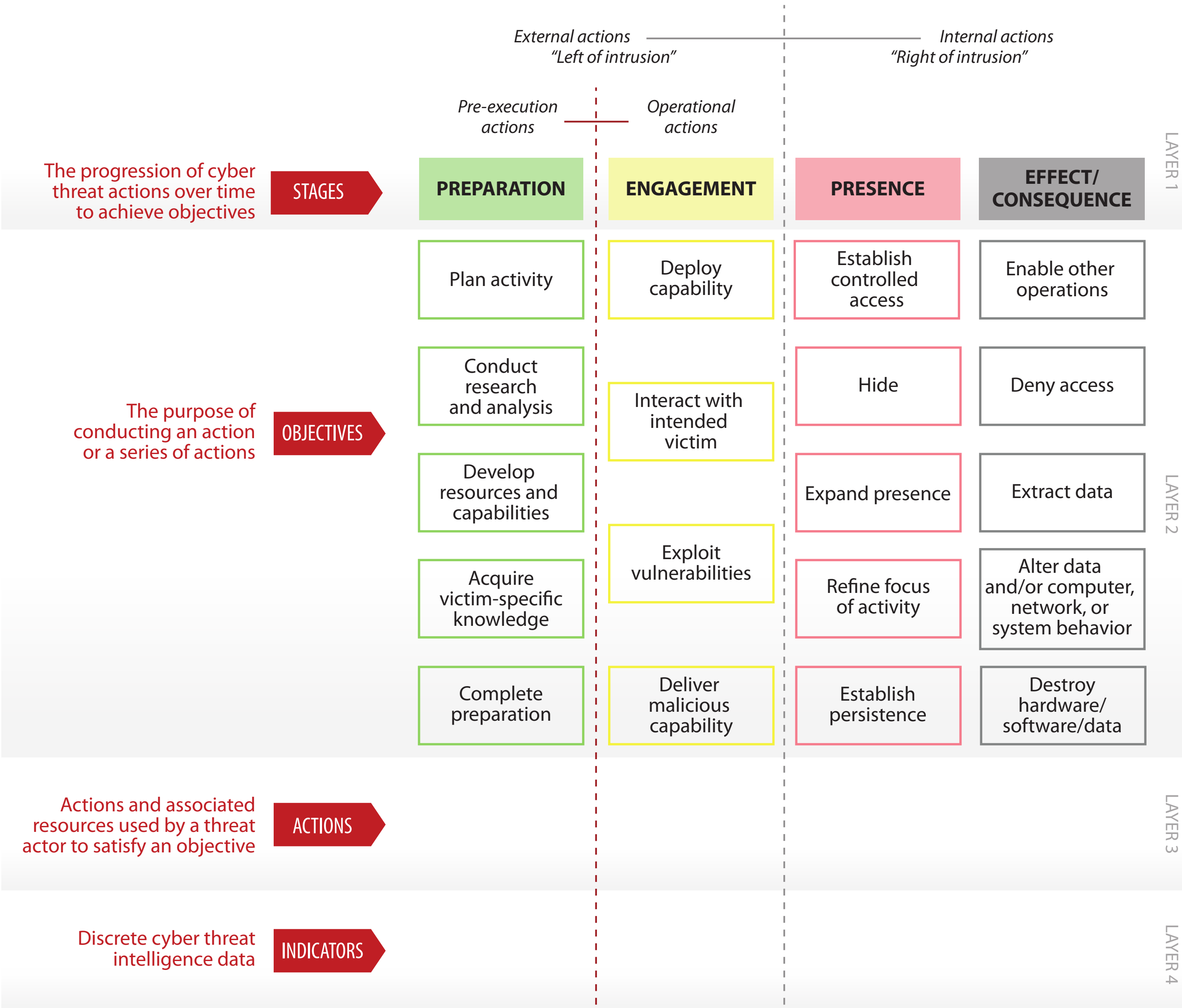

Figure 2. ODNI Cyber Threat Framework

industrial control system networks and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing attack capabilities, and—ultimately—executing the attack. Evidence of an adversary's position along this kill chain could help support decision-making on the imminence of potential attacks, with the final phases posing the most proximate indications that an adversary is poised to strike the grid.

Potential Attack Consequences

The imminence of an attack provides only one possible criterion for declaring a grid security emergency. A second would be the potential consequences of the attack. Indeed, when Congress defined grid security emergencies in the FPA, legislators established at least implicit, consequence-based thresholds for declaring an emergency. The FPA defines grid security emergencies as occurring when attacks that are imminent or under way "could disrupt the

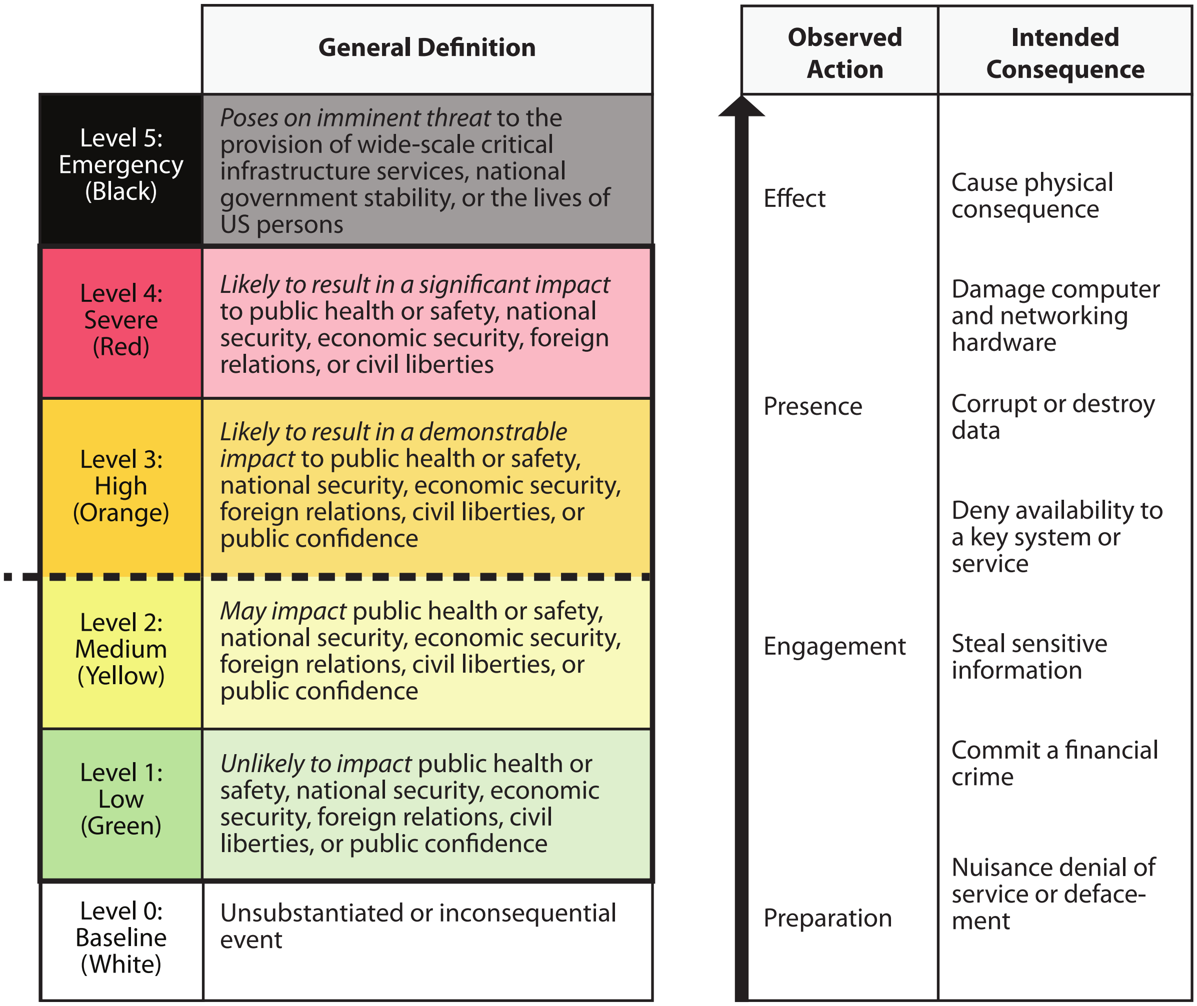

Figure 3. Elements of the Cyber Incident Severity Schema

operation" of devices or networks that are "essential to the reliability of critical electric infrastructure or defense critical electric infrastructure."[86]

However, the FPA does not clarify the extent of disruption that should trigger the declaration of an emergency. Some grid resilience stakeholders have expressed concern that policy makers might set the threshold too low, and declare grid security emergencies for minor incidents. For example, the ISO/RTO Council proposes that the use of emergency orders in such an emergency "should be reserved for true widespread emergencies."[87] But neither Congress nor DOE have yet specified what higher-level thresholds might be appropriate.

One approach to account for the potential consequences of an attack would be to leverage existing federal criteria for categorizing cyber events by the severity of their effects. The definition of "significant cyber incidents" in Presidential Policy Directive 41, *United States Cyber Incident Coordination*, provides a starting point to do so. Under the directive, significant cyber incidents are those that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or

[86] 16 U.S.C. § 824o–1, (a)(7).

[87] Paradise et al., "ISO-RTO Council Comments," 2.

public health and safety of the American people."[88] Policy makers could apply this demonstrable-harm standard to support decisions on whether to declare a grid security emergency. If officials determine that a cyber attack is likely to inflict such harm, their finding would provide a compelling justification for making an emergency declaration.

The December 2016 *National Cyber Incident Response Plan*'s cyber incident severity schema offers a still more detailed basis to assess attack consequences. The schema (Figure 3) serves as "a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments" and agencies.[89] Policy makers could use the schema to help develop consequence-based criteria for declaring grid security emergencies. For example, if assessments suggest that an attack is likely to create a "level 5 emergency," which poses "an imminent threat to the provision of wide-scale critical infrastructure services, national [government] stability, or to the lives of U.S. persons," the declaration of a grid security emergency should be near-automatic. Level 4 events would also be very strong candidates for justifying such declarations. However, as with all such criteria, the president should also retain the latitude to make declarations for less severe incidents (for example, the disruption of a cluster of major defense installations).

One advantage of leveraging these government-wide standards is that doing so can help integrate decisions on grid security emergencies into the broader US system for incident response. As officials update the *National Cyber Incident Response Plan* and its supporting severity schema, valuable opportunities will emerge to ensure that grid security emergency declarations and operations are part of a broader, multisector approach to strengthening infrastructure preparedness.

Grid-Specific Criteria for Assessing Attack Consequences: Building on Standards for Adequate Levels of Reliability

If policy makers rely only on general, government-wide decision criteria, they will miss opportunities to take advantage of the electric industry's standards for assessing the severity of threats to grid reliability. NERC has carefully defined what constitutes adequate reliability for the power grid, as well as the types of large-scale reliability failures that owners and operators need to prevent. If utilities and government agencies have the data and analytic tools necessary to determine whether adversaries' attacks will create such failures, their assessments could provide valuable input into decisions on declaring grid security emergencies.

The 2003 Northeast blackout spurred NERC's efforts to define adequate levels of grid reliability and specify the types of system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over wide areas of the United States and Canada, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The 2005 amendments required FERC to certify an electric reliability organization, which will have "the ability to develop and enforce . . . reliability standards that provide for an adequate level of reliability of the bulk-power system."[90] However, the FPA never defined *adequate level of reliability*; that task was left to the electric reliability organization.

When NERC became the electric reliability organization in 2006, defining the adequate level of reliability was one of its first initiatives. NERC's board of trustees approved an initial definition for the "characteristics of a system with an adequate level of reliability" in 2008, which was updated in 2013.[91] Three components of NERC's definition—cascading failures, uncontrolled separation, and instability—are

88 Obama, *United States Cyber Incident Coordination*.

89 DHS, *National Cyber Incident Response Plan*, 29–30.

90 16 U.S.C. § 824o, (c)(1).

91 NERC, *Technical Report*, 17.

especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS.[92]

The sections that follow examine these three components, the reliability failures they can entail, and implications for declaring grid security emergencies. Subsequent portions of the report analyze options to develop emergency orders tailored to prevent such failures. However, in grid security emergencies, risks of all three types of failures might emerge in rapid succession and would be inextricably linked.

Cascading failures. NERC defines cascading as "the uncontrolled successive loss of system elements triggered by an incident at any location." Such cascading "results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies."[93] NERC's definition states that a system is adequately reliable if the system will not experience cascading failures when struck by lightning or affected by other frequent, predictable incidents (i.e., "predefined Disturbances"). But more severe events have caused instabilities that led to cascading in the past and may do so again—especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout illustrates the speed with which failures can cascade. That blackout, which affected approximately fifty million people across the United States and Canada, started with a relatively minor incident. On a hot day in August, multiple 345-kilovolt transmission lines tripped after sagging into overgrown trees. With proper situational awareness, operators might have been able to take actions to handle such a contingency, but failures in the utility's control room alarm processor resulted in operators being entirely unaware of the problem. In an unfortunate coincidence, the utility's reliability coordinator also had computer problems and lacked the visual tools necessary to support grid operators.[94] These failures shifted power flows to a system of 138-kilovolt lines, which were unable to handle the added current flows, and overloaded the last remaining 345-kilovolt path into the area, beginning the major, uncontrollable cascading sequence.[95] This sequence tripped over five hundred generating units and four hundred transmission lines in only eight minutes—with most of these failures occurring *in the last twelve seconds* of the cascade.[96]

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversarial attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying critical generation and transmission nodes; alter protective relay settings so that grid components trip offline (or fail to do so) in ways that intensify the outages; deny grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and take other measures designed to produce cascading failures.[97] Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe—particularly by denying or corrupting situational awareness data.

The imminent danger or occurrence of adversary-induced cascading outages could be a criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt

92 See section 215 of the FPA, which defines *reliable operation* 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." 16 U.S.C. § 824o, (a)(4).

93 NERC, "Informational Filing," 1, 7.

94 NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

95 NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

96 NERC Steering Group, *Technical Analysis of Blackout*, 109.

97 Cherepanov and Lipovsky, "Industroyer"; Sistrunk, "ICS Cross-Industry Learning"; "Alert (TA17-163A)"; and Dragos, *CRASHOVERRIDE*, 24.

the operation of grid devices and networks essential to critical and defense critical electric infrastructure—on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

Uncontrolled separation. NERC defines uncontrolled separation as "the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss."[98] Severe events "resulting in the removal of two or more BES elements with high potential to cascade" can produce uncontrolled separation.[99]

Uncontrolled separation almost always occurs in conjunction with cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands that "quickly became unstable after the massive transient swings and system separation" because there was insufficient generation within the islands to meet electricity demand.[100] Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.[101] In the 1982 West Coast blackout, loss of 500-kilovolt lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, dividing the system into four unplanned islands.[102] A similar blackout in the same region in 1996, triggered by multiple major transmission line outages, again separated the Western Interconnection into four electrical islands "with significant loss of load and generation."[103] The onset of adversary-induced uncontrolled separation would provide a clear-cut basis for declaring the existence of a grid security emergency, if cascading failures had not already prompted the president to make such a determination.

Instability. NERC defines system instability as "the inability of the Transmission system to remain in synchronism . . . characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES."[104] The BES can experience frequency, voltage, or angular instability—though none should occur during normal operating conditions.[105]

Severe natural hazards and other disturbances can create temporary instabilities. Grid protection systems and operational protocols typically mitigate their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, the transmission system may experience large power swings if BPS generators accelerate or decelerate too much during a disturbance, causing transmission lines to trip and generators to go out of step and trip offline, and resulting in further acceleration and deceleration—or both.[106] Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread cascading failures. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur. Corrupting or disabling protection systems could also make critical grid components vulnerable to physical damage from enemy-induced power surges.

98 NERC, "Informational Filing," 6.

99 NERC, "Informational Filing," 13.

100 U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 75.

101 U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 104.

102 U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 105.

103 U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 106.

104 NERC, "Informational Filing," 6.

105 NERC, "Informational Filing," 1–2.

106 NERC, "Informational Filing," 6.

Evidence that adversaries were taking preparatory measures to create widespread instabilities could help the president determine that a grid security emergency exists.

However, it may be difficult to predict whether an impending attack will create such failures. The first requirement to do so will be to determine the extent to which adversaries have embedded advanced persistent threats or established other means of attack across the grid—a task that adversaries will complicate by attempting to hide their malware from detection. The next step will be to rapidly characterize these threats, assess the vulnerability of utility systems to them, and predict the consequences for grid reliability if the enemy strikes. Such assessments will also need to account for system-wide effects involving the interaction of multiple adversary-induced disruptions, which may compound and reinforce instabilities in ways that are difficult to predict. PJM Interconnection, LLC, the regional transmission operator for much of the Mid-Atlantic and some neighboring states, recently noted that "additional study is needed to better understand the expected impacts of a large-scale cyber-attack."[107] Given these challenges, it may be difficult to fully predict the potential impact of cyber attacks on grid reliability until attacks are well under way.

But it could also be risky to wait until attacks are occurring to declare a grid security emergency. In the 2003 Northeast event, for example, cascading blackouts spread across vast areas in seconds. If the president delays declaring a grid security emergency until cascades are under way, emergency orders designed to help prevent their spread may come too late. A better option might be to make an early decision based on imperfect assessments, especially if (as this report recommends) DOE can issue preattack emergency orders that will bolster grid defenses without disrupting normal electric service.

[107] PJM, "Comments and Responses," 35.

In particular, the president could consider declaring a grid security emergency if (1) an attack appears to be increasingly likely, and (2) assessments indicate that the impending attack may create cascading blackouts or other widespread instabilities. Figure 4 illustrates one option for developing a decision support framework that accounts for the likelihood and potential consequences of an attack. The vertical axis depicts the ODNI cyber threat framework's four stages of adversary actions, from potential attack preparations to actual strikes against the grid. An adversary's sudden, large-scale moves up this axis—especially in the context of a severe international crisis—could help the president determine that an attack is impending. The horizontal axis represents the risk that if an attack occurs, the grid will experience cascading failures and other widespread instabilities that would inflict demonstrable harm to national security, the economy, or public health and safety. Attacks that pose little or no risk of cascading blackouts might not warrant the declaration of a grid security emergency.

However, systemic threats to grid reliability are far from the only consequence-based criteria that the president might want to consider. More narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security, such as the National Capital Region, might be sufficient to declare a grid security emergency. Policy makers could develop more refined decision frameworks to account for a broad array of consequence thresholds, as well as further criteria for assessing attack imminence.

Data Sharing and Consultations with Industry

The electric industry can provide data and analytic support to help the president and other officials decide whether to declare a grid security emergency. Power companies will have direct access to the malware that adversaries implant on their networks, and will be well positioned to assess the potential

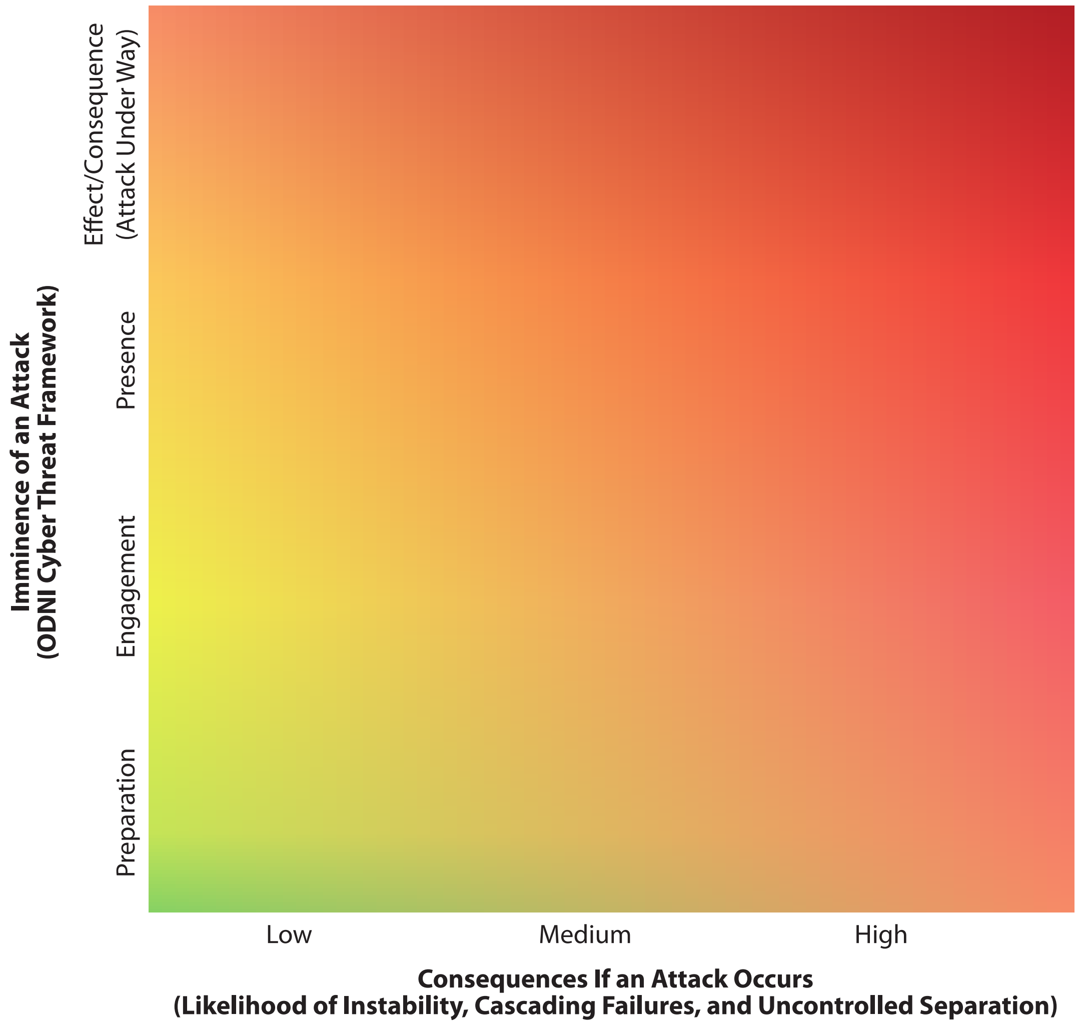

Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies

impact of various attack vectors on their systems and on the grid as a whole.

Government agencies and cyber contractors can help utilities target searches for this malware and provide additional value for the declaration process. If a regional crisis or other geopolitical factors increase the risk of cyber attacks on the grid, agencies should be prepared to ramp up information sharing with BPS entities, especially in terms of specific signatures or other threat indicators to search for in utility networks, logs, and critical equipment.

Industry and government should also explore how ongoing threat detection and analysis initiatives could directly help assess the imminence and potential consequences of attacks. For example, DOE has projects under way to bolster situational awareness for operational technology networks that could be applied to support such assessments. The department is developing capabilities to monitor traffic on operational technology networks via the Cybersecurity for the Operational Technology Environment project.[108] Other department-funded projects could prove useful for the emergency declaration process as well.[109]

108 DOE, *Multiyear Plan*, 23.

109 See, for example, the Containerized Application Security for Industrial Control Systems, Survivable Industrial Control Systems, and Research Exploring Malware in Energy Delivery Systems projects. "Sandia's Grid Modernization Program

Utilities and DOE might also refine ongoing information sharing initiatives to directly support the emergency declaration process. For example, DOE's Cybersecurity Risk Information Sharing Program is a public–private partnership to build bidirectional situational awareness and facilitate classified and unclassified information sharing.[110] DOE's 2018 cybersecurity plan launched additional activities to advance industry participation in the program, as well as its analytic tools and capabilities.[111] The program is managed by NERC and the E-ISAC, which play an integral role in sharing information and establishing situational awareness within the electricity subsector.[112] In addition, FERC recently issued a proposed directive for NERC to expand reporting requirements for cyber incidents, including for those that "might facilitate subsequent efforts to harm the reliable operation of the bulk electric system."[113] All of these efforts could be integrated to support assessments of the likelihood and potential consequences of attacks.

DHS's May 2018 cybersecurity strategy provides a broader approach to expand information sharing. Most important, the strategy could enable data from other infrastructure sectors to support the declaration process, especially from communications systems and other sectors that support power restoration operations. The strategy also calls for the expansion of automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders.[114]

Such automated sharing mechanisms will be vital to accelerate the identification and assessment of malware that could pose imminent threats to grid reliability. DHS's Automated Indicator Sharing capability "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."[115] This bidirectional information sharing will limit an adversary's ability to compromise multiple systems with the same malicious code. The Defense Advanced Research Projects Agency is also working on new technologies to protect the grid. In particular, the agency's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is working with companies to develop prototype capabilities for improving attack detection, response, and forensics support.[116] Moreover, as automated malware detection and analytic techniques improve, utilities may be able to speed their evaluation of potential intrusions and slash the number of false positives that current detection systems generate.[117] All of these initiatives should be leveraged to help the president determine whether to declare a grid security emergency.

Policy makers should also consider preplanning to consult with grid owners and operators in the declaration process. The FPA leaves the president with sole authority to declare a grid security emergency. If a potential emergency surfaced, the president would almost certainly draw on the expertise and recommendations of the secretary of energy, as well as other members of the National Security Council and supporting agencies. But power companies and their industry organizations will also have perspectives on operational and technical issues that could prove valuable for assessing potential attacks.

Newsletter," Sandia National Laboratories; and "REMEDYS," Cyber Resilient Energy Delivery Consortium.

110 "Energy Sector Cybersecurity Preparedness," DOE.

111 DOE, *Multiyear Plan*, 23.

112 "Electricity Information Sharing and Analysis Center," NERC.

113 FERC, *Cyber Security Incident Reporting Reliability Standards* (161 FERC ¶ 61,291), 2.

114 DHS, *Cybersecurity Strategy*, 13.

115 "Automated Indicator Sharing (AIS)," US-CERT.

116 Douris, "DARPA Research."

117 Ucci, Aniello, and Baldoni, "Survey on Machine Learning," 1:5; McElwee et al., "Deep Learning"; and McElwee, "Probabilistic Cluster."

Neither the FPA nor the grid security emergency rule explicitly provide for consultations with industry on whether to declare a grid security emergency. The FPA calls for consultations "to the extent practicable" before the secretary issues emergency orders.[118] But there are no equivalent provisions to include industry input in the emergency declaration process.

Industry and government partners should explore options to provide for such consultations, preferably by leveraging existing mechanisms under the ESCC and E-ISAC. As with consultations on issuing orders, urgent circumstances could shorten or preclude opportunities for government dialogue with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of "bolt from the blue" attacks. Nevertheless, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be invaluable for determining whether (and when) to declare a grid security emergency.

Grid Security Emergency Phases and Order Design Options

DOE and its industry partners should consider designing emergency orders for three potential phases of grid security emergencies. First, if the president determines that there is an imminent danger of an attack, the secretary should be ready to issue preattack orders that help utilities protect grid reliability. Second, once attacks are under way, the secretary could issue orders to reduce the risk of cascading failures or other widespread disruptions of electric service. Third, as utilities begin to restore grid reliability, orders could help utilities replace damaged equipment and counter adversary efforts to disrupt restoration operations.

Orders for each phase of a grid security emergency will differ not only in terms of when the secretary would issue them but also in the degree to which they will disrupt normal electric service. Some orders, such as staffing up emergency operations centers before an attack occurs, would leave customers unaffected. In contrast, orders for prioritized load shedding could temporarily halt service to many customers—but could also greatly reduce the risk that instabilities will lead to cascading blackouts.

Figure 5 provides examples of orders that vary in the degree of disruption they would inflict on normal service, and also in the way they would meet the phase-specific challenges of grid security emergencies. The analysis that follows examines each of them (and other possible orders) in greater detail.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, emergency orders for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are under way. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies "stop the bleeding" from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are under way.[119] Adversaries may also launch follow-on attacks once utilities begin focusing on restoration. Emergency orders to help utilities repel such attacks could become essential components of the restoration process.

[118] 16 U.S.C. § 824o–1, (b)(3).

[119] In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is fully restored to pre-event conditions) as the "new normal"—characterized by "degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months." See Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

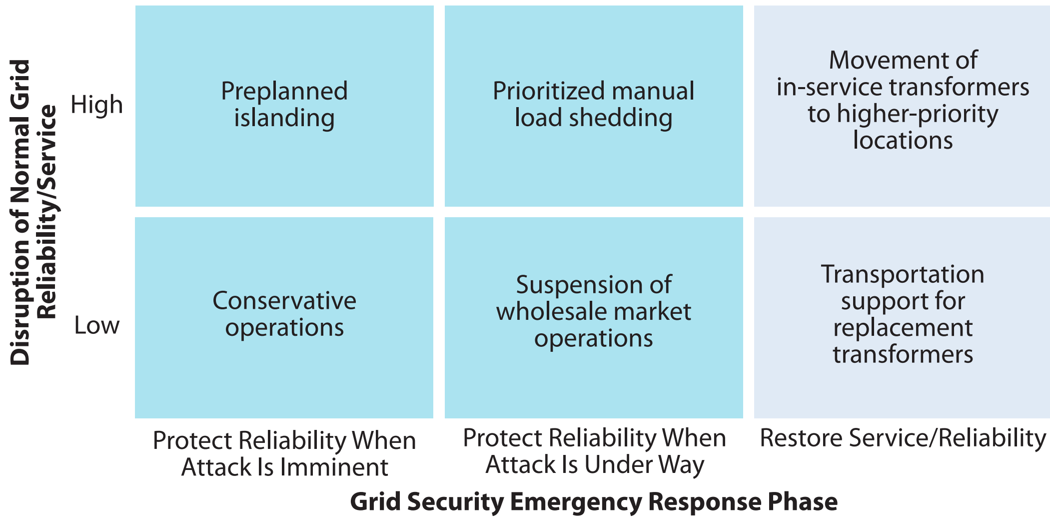

Figure 5. Emergency Order Matrix: Examples of Order Designs

DOE and its partners will need flexibility to deal with the overlapping phases of grid security emergencies. Nevertheless, being able to categorize potential orders in terms of when they would likely be issued and which phases of emergency operations they could support can help establish a systematic process for developing orders.

Creating emergency orders for all three phases can also help utilities and DOE integrate the orders into seamless, multiphase operational plans for grid security emergencies. As intense regional crises or other events elevate the risk of attacks on the grid, it will be prudent to preplan for the issuance of emergency orders for multiple grid security emergency phases. Orders for preattack measures such as conservative operations would be issued first if attacks are deemed imminent. At the same time, however, DOE and the utilities subject to emergency orders should be using any available warning time to prepare for the issuance and implementation of orders for the midattack and restoration phases.

Preattack Options

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal with these ambiguities is to delay the declaration of a grid security emergency until blackouts begin; doing so would forego the benefits of issuing preattack emergency orders. It may be possible to develop orders that will offer significant benefits if adversaries strike yet also have little or no impact on normal service—thereby offering "no-regrets" options to employ when the likelihood of an attack remains uncertain. Industry and government partners should also explore options for the preattack phase that would be more disruptive but also offer potentially far-reaching benefits. These two options occupy the left-hand column in Figure 5.

Conservative operations that utilities employ against natural hazards provide a model for protecting the grid in ambiguous preattack situations. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects and prepare for possible response and restoration operations if grid infrastructure is damaged.[120] For

[120] Conservative operations are not defined in the NERC glossary of terms. However, many reliability coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken to "implement

example, reliability coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.[121] Power companies may also cancel noncritical generation and transmission maintenance activities; reduce transfer limits to give the transmission system extra "slack"; and staff their backup control centers, critical BPS substations, and other vital facilities to set the stage for emergency operations as hurricanes approach.[122]

A defining feature of these frequently used conservative operations is that they do not disrupt normal service to customers. Their negligible service impact makes them more viable to implement when the storm's path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the US coast. Instead, they provide a wide "cone of uncertainty" that becomes increasingly narrow as the hurricane approaches. Utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other conservative operations. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these operations do not affect normal service to customers enhances the willingness of utility leaders to order their implementation while the storm track remains uncertain.

additional actions to ensure the BES remains reliable in the face of the additional threats" when "events, conditions, or circumstances may put the Bulk Electric System (BES) at an increased level of risk, compared to normal operating conditions." See PJM, "Conservative Operations," 3. Similarly, the Western Electricity Coordinating Council, defines conservative systems operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets "are restricted and managed in order to maintain or restore reliability of the power system from the negative influence of a triggering event or condition." See Western Electricity Coordinating Council, "Conservative System Operations," 4.

121 PJM, "Conservative Operations," 3.

122 PJM, "Conservative Operations," 9.

Industry and government partners should borrow from this model to develop orders for preattack conservative operations against cyber and/or physical attacks. Some have already begun to do so. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting conservative operations to meet the specialized challenges posed by cyber and physical threats.[123] This preparation will be extremely helpful as potential attacks loom. As a regional confrontation or other precipitating crisis intensifies, it is conceivable that the US intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. However, it is much more likely that ambiguities will persist about whether the adversary will actually attack and risk a devastating US response. To ensure that sufficient time is available to implement conservative operations, the secretary may need to order the initiation of such measures when enemy intentions remain uncertain—and when warning indicators may turn out to be false.

Many of the conservative operations that will bolster resilience against adversary attacks would be similar to those developed for natural hazards. For example, preattack emergency orders might direct BPS entities to increase generation reserves and/or re-dispatch resources out of least-cost operations. Other orders might be threat specific: for example, to intensify scrutiny of operational technology networks for malware and implement government-vetted countermeasures in ways that give utilities sufficient latitude to account for their unique system characteristics.

The common denominator for all such options: if the secretary issues orders for BPS entities to adopt conservative operations and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented the orders.

123 See, for example, PJM, *PJM Manual 13*, 73; Lucas, "Conservative Operations"; and SERC, *Conservative Operations Guidelines*.

However, because so many utilities already have robust plans and capabilities to protect their systems from imminent threats, close government–industry coordination will be required to ensure that emergency orders actually assist grid defense rather than function as speed bumps or useless distractions. Reliability coordinators and other grid operators serve as the pointy end of the spear for protecting grid reliability. Mandatory NERC standards require BPS entities to maintain voltage stability, automatic load shedding schemes, and contingency reserves for disturbances.[124] NERC standards also require transmission operators to "develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area."[125] Balancing authorities have similar requirements to manage generating and demand-side resources in their service areas.[126] These plans are exercised, tested, and frequently updated to bolster their effectiveness for actual emergencies. While many of NERC's mandatory standards apply when disturbances begin to occur, BPS entities are spring-loaded to implement conservative operations the moment potential hazards begin to emerge.

If major grid disruptions occur, BPS entities will not sit on their hands and wait for the president to declare a grid security emergency and the secretary to issue emergency orders. Indeed, DOE does not contemplate that they will. In the final grid security emergency rule, the department states that the declaration of a grid security emergency "does not preclude electric utilities from taking time-sensitive action to secure the safety, security, or reliability of the electric grid prior to the issuance of an emergency order."[127]

DOE and its partners can design emergency orders to help supplement and support such industry-led operations. For example, government agencies may acquire highly classified indicators that an attack is imminent. Declaring a grid security emergency and issuing emergency orders for conservative operations could ensure that utilities bolster their preparedness against such attacks on a consistent, nationwide basis, including those utilities that had not yet identified a need to act. Orders to help power companies ramp up and target searches for specific types of malware could supplement utilities' defensive operations as well. The secretary might also issue orders to ensure that such industry operations benefited from the FPA's regulatory protections and cost-recovery provisions.

More Disruptive Preattack Options

Many utilities are also prepared to take pre-event emergency measures that will significantly disrupt normal electric service, yet also offer benefits far beyond those that conservative operations can provide. For example, power companies can selectively halt electric service on warning of catastrophic storm surges. If seawater hits systems that are still carrying electricity, transformers and other difficult-to-replace grid components will suffer catastrophic physical damage. In 2012, weather forecasters warned that Superstorm Sandy might produce storm surges that would inundate critical substations and underground electrical equipment in lower Manhattan. Consolidated Edison's team made the politically difficult decision to prevent such damage by preemptively cutting of power to the area. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.[128] Moreover, Consolidated Edison limited the shutdown's disruptiveness by notifying customers hours earlier that the utility might halt service and by already having plans in place to prioritize the

[124] See, for example, NERC, *VAR-001-4.2*; NERC, *Standard PRC-006-3*; NERC, *PRC-010-2*; and NERC, *BAL-002-2(i)*.

[125] NERC, *EOP-011-1*, R1.

[126] NERC, *EOP-011-1*, R2.

[127] DOE, "RIN 1901–AB40," 1177.

[128] Miller, "Con Edison Shuts off Power."

restoration of service to hospitals, water-pumping stations, and other critical facilities.[129]

BPS entities continue to use "shutdown on warning" as an effective tool to avoid equipment damage against severe weather and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent equipment damage and speed up restoration. Generation owners similarly chose to shut down or evacuate some generating units in the storm's projected path.[130]

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and heating and air conditioning systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

DOE and its electricity subsector partners should consider developing emergency orders that offer a similar set of risks and rewards. However, doing so will entail problems beyond those associated with protecting the grid against natural hazards. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an adversary will actually pull the (cyber) trigger and whether attacks are likely to cause demonstrable harm to the US economy, national security, or public health and safety. Measures developed for natural hazards may also offer uncertain benefits against imminent cyber and physical attacks. For example, further analysis will be required to determine whether and how preattack grid shutdowns might help counter specific cyber threats, including attacks that disable protection systems to facilitate equipment-damaging power surges.

Other disruptive emergency orders could counter a broader range of threats but entail major (and perhaps insurmountable) problems for nationwide employment. The upper left-hand box in Figure 5 offers a prime example of such options: preplanned power islanding. Microgrids offer the most familiar means of establishing power islands.[131] A growing number of military bases, universities, and major hospitals have sufficient generation and other electric infrastructure on-site so that if adversaries black out the surrounding grid (or pose an imminent danger of doing so), those facilities can separate from the grid and operate independently as power islands.

However, microgrids do not offer "bulletproof" power resilience. Cyber adversaries are sure to treat on-base electric infrastructure, including renewable generation assets, as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas–fired generators, the power they provide is only as resilient as the gas transmission and distribution systems that supply them—and cyber threats to natural gas systems are rapidly escalating.[132] Moreover, building microgrids requires extensive investment in grid infrastructure. Investment demands will be especially heavy if installations want to serve not only the critical loads within their perimeters but also the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to building microgrids, power companies are also analyzing ways to establish emergency power islands with less infrastructure investment. One particular option being explored by GridEx participants is to preplan to establish large

[129] DiSavino and Sheppard, "ConEd Cuts Power."

[130] NERC, *Hurricane Harvey*, v.

[131] DOE's definition of microgrids: "A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously." "The Role of Microgrids," DOE.

[132] DOE, *Quadrennial Energy Review*, 7-7; and Parfomak, *Pipelines*, 2–3.

power islands by using existing grid infrastructure within their boundaries. Utility personnel have noted that they might be able to use legacy balancing areas as a starting point to establish island boundaries. On warning of an imminent attack or under other extraordinary circumstances, utilities would separate a power island from the surrounding grid and operate independently to serve critical loads within it. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, preplanned islands might become a hedge against cascading failures and uncontrolled separation.

In practice, preplanned islanding will be practical only if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for preplanned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands to enable them to function independently of the grid. Moreover, standing up islands would severely disrupt day-to-day service for noncritical customers and create instabilities for surrounding systems that could produce additional service disruptions. Accordingly, preplanned islanding might be considered a "huge-regrets" emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created.

DOE and its industry partners should also consider developing preattack emergency orders that fall between the two extremes of no-regrets options and highly disruptive measures. For example, to avoid remote execution of destructive malware on utility networks, orders might direct utilities to disconnect their systems from the internet. Utilities could also take additional measures to isolate or compartmentalize all control systems. Implementing these measures would curtail potential attack vectors, but would do so at a price. Disconnecting from the internet would hobble wholesale market operations, disable email as a basic communications tool, affect an entity's access to other means of communications (i.e., E-ISAC and DOE portals), impact an entity's ability to comply with regulatory requirements, and produce other undesirable consequences. Any unexpected challenges in isolating or compartmentalizing the control systems that are critical to the functioning of the grid could also jeopardize normal service. Nevertheless, if industry and its government partners can preplan to anticipate and overcome these challenges, even highly disruptive preattack options may be useful to protect the grid from cascading failures.

Extraordinary Measures when Attacks Are Occurring

Emergency orders when attacks are under way can help utilities prevent widespread instabilities, cascading failures, and uncontrolled separation. Under the auspices of the ESCC, utilities and their resilience partners are already developing "extraordinary measures" to operate the grid if adversaries disable or corrupt SCADA (supervisory control and data acquisition) systems, state estimators, and other operational technology hardware and software components on which utilities typically rely.[133] For example, the North American Transmission Forum is leading an initiative on supplemental operating strategies to help power companies manually cope with the loss of energy management systems and/or SCADA across a large geographic footprint.[134]

---

[133] These extraordinary measures include resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary backup systems, and development of supplemental operating strategies use in "degraded states." See "ESCC: Electricity Subsector Coordinating Council," ESCC.

[134] Galloway, "Advancing Reliability and Resilience of the Grid," 2.

These industry efforts provide a basis to develop grid security emergency orders for extraordinary measures when attacks are under way. So, too, do existing BPS emergency operating plans, capabilities, and operational requirements to manage the grid instabilities. Options for such orders vary in terms of the disruption they would inflict on normal grid operations.

Figure 5 provides an example of a low-disruption order for this phase: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate needs or for the next day). These entities have taken extensive measures to keep market functions separate from their operational control of the grid. Many entities also have mechanisms in place to operate when markets are temporarily suspended. Over extended periods, however, cyber attacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, undercut the valuation of power companies on Wall Street, and magnify the damage to the US economy that attacks on the grid will create.

Regional transmission organizations are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the transmission operator[135] for the Mid-Atlantic and other US regions, has called for the development of mechanisms to permit "nonmarket" operations in extreme circumstances.[136] A number of options exist to provide for such operations. For example, if the secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell power at a fixed price predetermined by DOE.[137] Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high-benefit/low-disruption emergency orders, including orders for maximum power generation when attacks are under way, will also fall into this category.[138]

Industry and government partners will also need to develop more disruptive emergency orders that can protect grid reliability in extraordinary circumstances. One option to do so involves operating an area in a generation-deficient state for a prolonged period, supported (when practical) by power imported from neighboring regions. The top center box of Figure 5 provides another prominent example: prioritized manual load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by selectively shedding load and implementing rotating blackouts.[139]

A failure to shed load contributed to the cascading failures in the major 2003 blackout. After-action reports from that event found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission

[135] The NERC glossary defines *transmission operator* as "the entity responsible for the reliability of its 'local' transmission system, and that operates or directs the operations of the transmission Facilities." *Transmission operator area* is defined as "the collection of Transmission assets over which the Transmission Operator is responsible for operating." See NERC, *Glossary*.

[136] PJM, "Comments and Responses," 6, 39–40.

[137] Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. PJM, "Comments and Responses," 39.

[138] Maximum generation involves increasing generation "above the maximum economic level" when additional generation is needed. See PJM, *PJM Manual 13*, 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see MISO, "MISO January 17–18 Maximum Generation Event Overview."

[139] Severe Impact Resilience Task Force, *Severe Impact Resilience*, 11.

lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. A US–Canada task force found that "timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio."[140] In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.[141]

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for transmission operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation for building emergency orders to reduce the risk that physical and cyber attacks will create cascading blackouts.

One way to shed load would be to order power companies to execute rotating blackouts. In such controlled outages, grid operators interrupt service on a rotating basis to sequential sets of distribution feeders for limited periods (typically twenty to thirty minutes).[142] Grid operators employed rotating blackouts to help protect grid reliability during the "Big Chill" that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT's rotating blackouts during the event affected a total of 4.4 million customers.[143] The temporary blackouts were no doubt disruptive. However, by reducing the risk of cascading failures, those outages offered compelling system-wide benefits for protecting reliability.

But rotating blackouts will not offer the best option for load shedding in all grid security emergencies. In the event of a massively disruptive attack, an emergency order might require utilities to shed load without implementing rotating blackouts, because such rotating outages could introduce unacceptable reliability risks during a chaotic and rapidly changing situation. As an alternative, utilities can implement "brownouts": that is, conduct voltage reductions to maintain a continual balance between supply and demand within a balancing area.[144] However, brownouts and rotating blackouts share a serious limitation: they affect all customers equally. But not all customers will be equally important in a grid security emergency. DOE and industry will need orders and implementation plans for manual, prioritized load shedding, so utilities can focus on sustaining power flows to hospitals and other critical loads while also reducing the risk of cascading power failures. NERC already requires BPS entities to have plans for both automatic and manual load shedding.[145] Utilities and DOE should use these requirements as the starting point to design emergency orders for extraordinary measures that would supplement what BPS entities are already prepared to do to if major instabilities occur.

Emergency Orders to Support Power Restoration

The rightmost column in Figure 5 provides the third category for emergency orders: those that can help grid owners and operators restore power after widespread

140 U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 147.

141 U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 77.

142 NERC, *Reliability Terminology,* 1.

143 FERC and NERC, *Restoration and Recovery Plans*, 61.

144 NERC, *Reliability Terminology*.

145 NERC standards currently emphasize automatic load shedding to protect grid reliability. See NERC, *Standard PRC-006-3*; and NERC, *PRC-010-2*. However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing emergency orders to prevent or mitigate cascading failures. See NERC, *EOP-011-1*.

outages occur. In past cascading failures of the US electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days (and in some cases much less time) because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators, transmission lines, and other system components are designed to trip offline when instabilities occur, thereby protecting them from damaging power surges—and leaving them available to help rapidly reestablish the flow of power.[146] However, if cyber or physical attacks destroy critical system components, requirements to repair or replace such assets could greatly lengthen and complicate the restoration of service. Emergency orders can support restoration operations and better align them with national-level priorities.

Emergency orders for the restoration phase can also account for the risk that adversaries may continue their attacks as power companies begin to restore service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to US military bases and other vital facilities and to seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeting power restoration operations can help adversaries achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply. Risks of reattack should help drive the design of restoration-phase emergency orders.

Advanced persistent threats hidden in utility networks will pose especially significant challenges for restoration. This malware may enable adversaries to conduct recurring attacks based on timing or network conditions. Unless utilities thoroughly eradicate such malware, repeated outages could impede restoration operations and put the grid at sustained risk of cascading failures.[147] Physical attacks against restoration personnel and replacement equipment in transit would pose additional problems. Grid security emergency orders can help utilities restore electric service even if they remain “under fire” from cyber and kinetic weapons.

Such orders will differ in the degree to which they could alter existing utility plans to restore power. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks, and barges) from where power companies store them to where they are needed as replacements.[148] Subsequent portions of this report examine how DOE could collaborate with other federal agencies and state and local officials to waive transportation regulations and bolster security support for such operations. The secretary could also issue orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, ports, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these prioritized customers. Emergency orders can help incorporate other national security–related assets that utility plans do not typically include, such as components of the defense industrial base essential for resupplying US forces abroad.

DOE and its industry partners should also create template emergency orders for in extremis restoration operations that would more sharply depart from existing industry plans and procedures. The upper right-hand box of Figure 5 offers an example

146 NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, 1.

147 Homeland Security Advisory Council, *Final Report*, 7.

148 DOE, *Strategic Transformer Reserve*, 12–13.

of one such option. If adversaries damage or destroy an extraordinarily large number of transformers, the secretary might order utilities to remove surviving in-service transformers in the same voltage class from their substation and transport them to serve vital national security facilities in the National Capital Region or other areas. Orders of this kind could create severe disruptions in existing service. They might even impede system restoration if utilities and their government partners have not adequately prepared to account for challenges regarding transformers' technical specifications and the BPS's overall configuration. However, if these challenges can be addressed, the benefits might be greater still for helping the United States defeat its adversaries.

Other in extremis orders could help utilities operate the grid if equipment damage is so extensive (or reattacks are so effective) that full system restoration will require many weeks or even months. The FERC/NERC study on severe impact resilience (May 2012) found that coordinated cyber and physical attacks may force the grid into a "new normal" state of "degraded planning and operating conditions" that could last for months or years, including reduced generation and transmission resources and planned and unplanned rotating blackouts.[149] DOE and power companies should consider how emergency orders and supporting regulatory waivers might help electric utilities serve priority loads and accelerate restoration under new normal conditions.

One option to do so is to preplan for the waiver of selected reliability standards. The *Severe Impact Resilience* study recognized that catastrophic events could "put entities in a position where they cannot comply with all standards." However, in part due to the difficulty of predicting the circumstances that entities will face, the study recommended against preplanning for waivers. Instead, the study proposed relying on entities to "'do the right thing' for reliability and public safety" and self-report violations as circumstances permit.[150]

NERC should reconsider this conclusion in light of the secretary's new grid security emergency authorities and the waiver provisions they entail. FERC, NERC, and their industry and government partners should identify specific regulatory waivers and related measures that could provide the basis for utilities' contingency planning for new normal operations.

One such option lies in reliability standards for managing unforeseen contingencies. Currently, NERC standards require BPS entities to operate in an N-1 state: that is, they must be able to sustain service even if they suffer the most severe single contingency (such as the loss of a single critical line, transformer, or generator) possible in their system.[151] Operators may be required to shed load prior to any contingency to maintain the N-1 state. These requirements apply during normal day-to-day operations as well as during system restoration.

Returning to an N-1 state in the face of coordinated cyber and physical attacks is likely to be a lengthy process involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. To help enable utilities to serve critical facilities during such sustained events, the secretary might issue emergency orders that explicitly allow utilities to function in an N-0 operating state (as long as doing so did not risk causing cascading failures or equipment damage).[152]

Issuing such orders could entail important benefits. Operating at N-0 would give utilities greater operating flexibility and ensure that entities can continue to serve as much load as possible during a grid security

[149] Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

[150] Severe Impact Resilience Task Force, *Severe Impact Resilience*, 17.

[151] NERC, *BAL-002-2(i)*, requirement R2; NERC, *TOP-001-3*, R12 and R14; and NERC, *IRO-008-2*, R5 and R6.

[152] For N-0, all elements must be within thermal and voltage limits prior to any contingency.

emergency, including military installations and other priority customers. Unlike under N-1 operations, entities would be required to shed load only prior to any contingency for the most severe single contingencies if any of those single contingencies would cause cascading failures, or after a contingency that required load shedding to eliminate overloads or low voltage.

But operating at N-0 would also entail significant risks. N-1 standards exist for compelling reasons: they help protect grid reliability against severe contingencies. Deviating from N-1 requirements will create greater risks of causing further blackouts in new normal conditions. Moreover, N-0 operations would require even greater coordination among BPS entities (including reliability coordinators, transmission owners, and local control centers), as a single outage could result in equipment overloads or voltage violations and require extraordinary mitigation measures. Accordingly, this option will be feasible only if DOE partners with FERC, NERC, and entities to fully understand and mitigate such risks, as well as maximize the potential benefits of N-0 operations for serving critical national security–related loads.

Additional Emergency Order Design Parameters and Supporting Initiatives

Adversaries will attempt to black out the US grid to achieve their broader political, economic, and military objectives in a conflict. Government agencies and the electricity subsector should design emergency orders to help prevent attackers from accomplishing their objectives, and—ideally—to help deter them from attacking at all.

However, deterring and defeating attacks on the grid will require resilience improvements beyond the electricity subsector. Attackers may simultaneously strike electric and communications systems to both disrupt the grid and impede the issuance and implementation of emergency orders. Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. Countering such efforts will require unprecedented collaboration among utilities, government agencies, media, and the broader telecommunications sector.

Designing and implementing emergency orders to blunt attacks by Russia, China, and other potential high-capability adversaries will place extraordinary burdens on electric utilities—burdens that few ratepayers and utility investors will be eager to bear on their own. To help power companies meet these challenges, it will be essential to fully leverage the regulatory waiver and cost-recovery provisions of the FPA, and examine whether Congress should expand these provisions as threats continue to intensify.

Deterring and Defeating US Adversaries

The US *National Security Strategy* emphasizes that cyber threats to US critical infrastructure are becoming increasingly severe. In particular, the strategy notes that cyber weapons "enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces."[153] Pairing cyber attacks with coordinated physical strikes against transformers and other critical grid infrastructure would exacerbate these disruptive effects.

The strategy identifies two primary means for deterring catastrophic attacks, both of which can be supported by emergency orders and implementation plans:

(1) Convince adversaries that they will suffer "swift and costly consequences" if they strike the grid or other US targets, and that the United States "can and will defeat them" if deterrence fails.[154]

[153] White House, *National Security Strategy*, 13, 28.

[154] White House, *National Security Strategy*, 28.

(2) Strengthen infrastructure resilience to create "doubt in our adversaries that they can achieve their objectives" if they do attack (i.e., deterrence by denial).[155]

Deterrence through Cost Imposition: Protecting Defense Critical Electric Infrastructure

In amending the FPA, Congress placed a particular emphasis on the need to protect the reliability of defense critical electric infrastructure (i.e., grid components that serve military bases and other facilities "critical to the defense of the United States" and vulnerable to the disruption of grid-provided electricity).[156] Emergency orders to protect such infrastructure can help ensure that US bases have the power they need to respond to attackers. But prioritizing defense installations for support in grid security emergencies will require deeper analysis of US deterrence requirements, given DOD's growing dependence on civilian assets and functions to execute defense missions. Deterrence by cost imposition will also depend on convincing potential adversaries that the United States will be able to identify them as the perpetrators of attacks on the grid. DOE and its industry partners should explore how emergency orders can facilitate attack attribution, as well as provide broader support for the credibility of the US deterrence posture.

A relatively small number of military bases are responsible for inflicting unacceptable costs on potential adversaries. The US Defense Science Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of US strike systems (cyber, nuclear, and nonnuclear) and supporting infrastructure to ensure "that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks."[157] Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which US strike systems rely and ensure that they have reliable power even in extended conflicts.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The strategy emphasizes that "we must convince adversaries that we can and will defeat them—not just punish them if they attack the United States."[158] Defeating adversaries in regional contingencies in the South China Sea, the Baltics, or other potential conflict zones will place special burdens on US grid resilience. US capabilities to conduct operations abroad are increasingly dependent on domestic military and civilian assets. In particular, a vast array of US defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy, operate, and sustain US power projection forces for regional conflicts.

This dependence makes the grid a prime target for attack. The DOD *Mission Assurance Strategy* notes that adversaries may seek to disrupt power projection capabilities by attacking the domestic infrastructure systems on which they depend. In particular, the strategy warns that "potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting

[155] White House, *National Security Strategy*, 13, 28. The literature on security studies defines deterrence by denial in a variety of ways. This report follows the definition used in the *National Security Strategy*, which is consistent with the definition employed in the Obama administration's deterrence policies. See Lynn, "Defending a New Domain." For broader studies of deterrence by denial, and critiques of the way in which the strategy employs the term, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy"; Mitchell, "Case for Deterrence by Denial"; Gerson, "Conventional Deterrence," 40; and Nye, "Deterrence and Dissuasion," 56–58.

[156] 16 U.S.C. § 824o–1, (a)(4).

[157] Miller and Gosler, "Memorandum." See also pp. 3, 6–7, 11–12, and 17–18 of the report.

[158] White House, *National Security Strategy*, 28.

critical defense and supporting civilian capabilities and assets," including the US power grid.[159]

Ensuring the availability of resilient power for ports and other civilian assets essential for power projection will require emergency orders to serve an expanded set of customers, far beyond those responsible for strike operations. These orders will also need to encompass a much larger array of defense critical electric infrastructure owners and operators.

Electric companies and defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds from separate high-voltage transmission substations to serve defense installations provides a valuable means of strengthening resilience against physical attacks.[160] Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.[161] Utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as power islands independent of the surrounding grid.[162]

While valuable, these initiatives do not eliminate the need to develop national defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases and will not necessarily provide resilience against cyber attacks (since even redundant feeds may share common cyber vulnerabilities). Emergency generators will break down in long-duration outages. Moreover, resupplying them with fuel will become increasingly difficult at installations that lack massive storage tanks. Large-scale microgrids for islanded operations can provide more resilient power. DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction and scale them to serve infrastructure loads outside the base that are essential for on-base operations. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for war fighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, including the intermodal transportation systems that help deploy and sustain US forces abroad.

DOE and its industry partners can design emergency orders to support US deterrence credibility and power projection capabilities far more quickly and with less infrastructure investment. However, for utilities to implement these orders, they must first know which customers are of the highest priority for sustaining and restoring service when enemies strike. Section 215A of the FPA provides the ideal starting point develop and share such data. The act requires the secretary of energy, in consultation with other federal agencies and grid owners and operators, to identify and designate "critical defense facilities" in the forty-eight 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 electric energy provided to such facility by an external provider."[163] Congress's definition of defense critical electric infrastructure also helps guide implementation of that requirement. Such assets include "any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]" as a critical defense facility, "but is not owned or operated by the owner or operator of such facility."[164]

159 DOD, *Mission Assurance Strategy*, 1.

160 ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39.

161 ASD(EI&E), *AEMR Report Fiscal Year 2016*, 40.

162 ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39. See also Van Broekhoven et al., *Microgrid Study*; and Marqusee, Schultz, and Robyn, *Power Begins at Home*, 13–15. A number of "islandable" microgrid projects are under way at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See McGhee, "EEI Executive Advisory Committee," 4; and Kaften, "DoD Tests Energy Continuity."

163 16 U.S.C. § 824o–1, (c).

164 16 U.S.C. § 824o–1, (a)(4).

DOE is already working with DOD to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD has a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.[165] However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure. Figure 6 illustrates how DOE, DOD, and their partners might categorize all such defense-related assets and the defense critical electric infrastructure that grid security emergency orders should help protect.

At the innermost core lie those installations and supporting infrastructure capable of inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital. Protecting the reliability of the defense critical electric infrastructure on which they depend should be the top nationwide priority for developing emergency orders and company-specific implementation plans.

The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining these assets abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the US grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. DOD is in the process of identifying the specific facilities and supporting infrastructure that are required to help execute operational plans around the globe.[166] The department also has well-established criteria and assessment methods to prioritize these supporting assets for risk mitigation.[167] DOD and DOE should use these tools to identify the broader set of defense critical electric infrastructure needed for deterrence

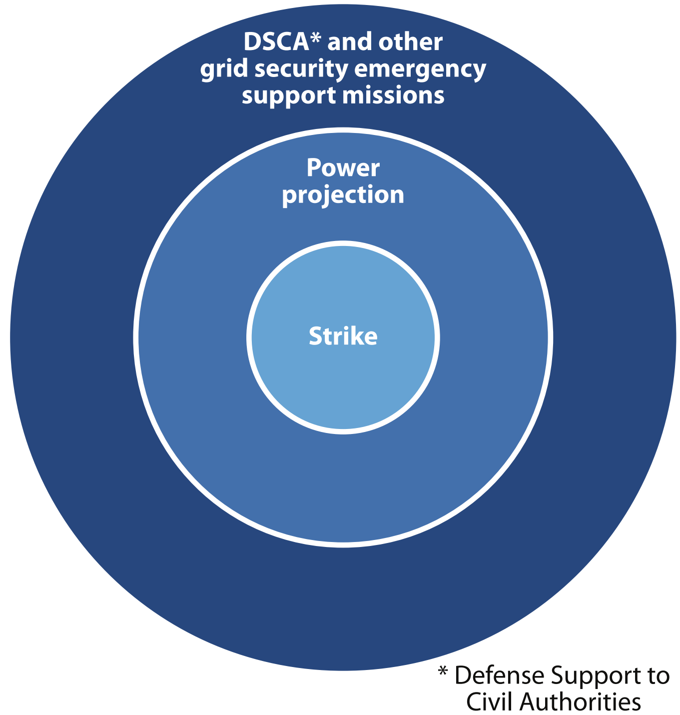

Figure 6. Categories for Protecting Defense Critical Electric Infrastructure

and to help power companies preplan to support critical assets within their service footprints.

The third circle includes the still larger array of defense installations, including National Guard bases, which would be essential for providing defense support to civil authorities if disruptions of the grid jeopardize public health and safety.[168] During Hurricane Maria (2017), Superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, lodging, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and delivering other assistance. Protecting or rapidly restoring the reliability of the defense critical electric infrastructure that supports

165 See DOD, *Manual 3020.45*; and DOD, *Directive 3020.40*.

166 DOD, *Directive 3020.40*.

167 DOD, *Manual 3020.45*.

168 Of course, many National Guard installations that could conduct defense support operations may also be responsible for assisting war fighting operations abroad, and would therefore fall within the second circle as well.

these defense-support-to-civil-authorities functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public.[169]

Building preparedness for grid security emergencies can also help meet an underlying challenge for deterrence: attack attribution. To convince foreign leaders that they will suffer swift and costly consequences if they strike the grid, those leaders must first believe that the United States will be able to identify them as the attackers.[170] The Federal Bureau of Investigation (FBI) and other federal agencies are improving their attribution capabilities.[171] US agencies also devote massive resources to human and technical intelligence collection on potential adversaries, which could further assist attack attribution.[172] Nevertheless, adversaries may seek to strike in ways that complicate attack forensics by employing wiper tools and using other tactics, techniques, and procedures to cover their tracks.[173]

Emergency orders can help defeat adversaries' efforts to evade attribution. By refining the FPA's information sharing mechanisms and building them into emergency orders, utilities and their government partners can strengthen their ability to share malware samples and other information on threat signatures.[174] New technologies can bolster such collaboration. For example, the Containerized Application Security for Industrial Control Systems project is designed to help grid operators isolate and capture malware on their systems, enabling samples to be shared with government agencies while still preventing that malware from disrupting system operations.[175]

Developing emergency orders and implementation plans to defend the grid can also provide broader support for attribution. James Miller notes that "while cyber hardening of US critical infrastructure will never be good enough to prevent a Russia or China from being able to threaten a major attack, it can cause them to have to be 'noisier' to do so, thereby boosting our confidence in attribution."[176] Emergency measures to protect grid reliability can complicate attack planning and, ideally, drive adversaries to strike in ways that will make them easier to identify.

Deterrence by Denial: Protecting Critical Electric Infrastructure

Convincing adversaries that they will suffer unacceptable costs if they strike the grid is only one means of deterring such attacks. Another means is to reduce the benefits that adversaries expect to achieve by attacking. In classical deterrence theory, both factors combine to influence an adversary's decision on whether to strike. As Joseph Nye Jr. puts it, "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."[177]

The *National Security Strategy* calls for measures that can prevent attackers from achieving the goals they seek and thereby strengthen deterrence by denial. The strategy states that "we must ensure the ability to deter enemies by denial, convincing them that they cannot accomplish their objectives through the use of

169 Countering such adversary efforts will also require protecting electric service to financial institutions, regional hospitals, and other civilian assets essential to the US economy and public health and safety. The next section of the report examines these requirements and their implications for deterrence and emergency order design.

170 On the tasks that attribution comprises, see Lin, "Escalation Dynamics," 49–50.

171 Smith, "Roles and Responsibilities." See also Newman, "Hacker Lexicon."

172 Miller, "Cyber Deterrence."

173 Newman, "Hacker Lexicon."

174 See 16 U.S.C. § 824o–1, (d). Later sections of this report provide a more detailed assessment of provisions for improved information sharing.

175 "Sandia's Grid Modernization Program Newsletter," Sandia National Laboratories.

176 Miller, "Cyber Deterrence."

177 Nye, "Deterrence and Dissuasion," 45.

force or other forms of aggression."[178] Ensuring that the grid and other infrastructure sectors can survive attacks and rapidly recover from service interruptions plays an especially important role in the administration's deterrence posture. The strategy notes that "a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives."[179] More recent statements of administration policy also note that deterrence by denial "must be foundational to the U.S. deterrence approach," and that US efforts must continue "to deny adversaries the benefits of their malicious cyber activities."[180]

Emergency orders and implementation plans may be able reduce the benefits that adversaries expect to achieve by attacking the grid. Preattack orders to bolster grid defenses can impede adversary efforts to disrupt grid reliability. Once attacks are under way, orders for prioritized load shedding and other extraordinary measures can help limit the damage the adversaries may hope to inflict on financial institutions, hospitals, and other electricity-dependent facilities. Orders that accelerate power restoration to these critical facilities may also reduce the effects of an attack, and thereby strengthen deterrence by denial.

The FPA is ready-made to support such improvements. In addition to protecting defense critical electric infrastructure, and thereby assisting deterrence through cost imposition, the act also authorizes orders to protect a much broader portion of the grid: critical electric infrastructure. Such infrastructure comprises grid systems or assets whose incapacity or destruction would "negatively affect national security, economic security, public health and safety, or any combination of such matters."[181] Orders to help utilities defend critical electric infrastructure can reinforce deterrence by denial—and, if deterrence fails, reduce the devastation that adversaries will create.

However, developing and implementing such orders will entail major challenges. Some deterrence theorists doubt whether deterrence by denial is practical in cyberspace, in part because offensive capabilities are so much stronger than cyber defenses. The conclusion of this report will examine those arguments and explore broader opportunities to bolster deterrence and help the United States defeat our adversaries if conflicts nevertheless occur. First, however, DOE and its partners will need to overcome two impediments to protecting critical electric infrastructure: determining which specific facilities and functions are truly critical, and securely sharing that information with utilities so they can refine their operational plans for grid security emergencies.

Building a "Section 9+ List:" Prioritizing Infrastructure for Sustainment and Restoration

Identifying and prioritizing critical electric infrastructure will be far more difficult than doing so for defense critical electric infrastructure. If adversaries create cascading blackouts across one or more interconnections, the disruption of many thousands of civilian-owned facilities could negatively affect national security, the US economy, and public health and safety. Utilities cannot possibly prioritize the flow of power to all such facilities. Government agencies and their private sector partners will need to determine which specific customers (and the critical electric infrastructure that serves them) are most vital to the nation and must continue to receive power if widespread instabilities occur.

Executive Order 13636 (February 2013) provides an existing methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the secretary of homeland security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident "could reasonably result in catastrophic regional or national effects on public health or safety, economic security,

178 White House, *National Security Strategy*, 28.

179 White House, *National Security Strategy*, 13.

180 DOS, *Recommendations*, 2.

181 16 U.S.C. § 824o–1, (a)(2).

or national security."[182] That standard—catastrophic damage—provides a useful criterion to identify the highest-priority assets and associated critical electric infrastructure for protection by emergency orders in grid security emergencies. Over time, orders and contingency plans could gradually encompass less-critical facilities and grid infrastructure.

Of course, the section 9 methodology and subsequent list were never intended to support the implementation of section 215A of the FPA. As a result, the section 9 methodology falls short of meeting all the requirements for supporting emergency order design. One gap lies in the threats that drive the selection of critical assets. Section 9 focuses exclusively on infrastructure at risk from cyber attacks. The FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on electric systems. Executive Order 13636's section 9 requirements also create a "corporate"-level list that is not broken down into the key assets within those corporations (i.e., facilities, systems, and nodes). More fine-grained data and analysis will be required to identify facilities for which sustained electric service will be most crucial. Efforts to prioritize grid service will also need to account for the increasingly complex interdependencies between US infrastructure sectors.[183]

Despite these shortfalls, Executive Order 13636's methodology can provide a valuable starting point for identifying the most vital critical electric infrastructure and supporting assets. DOE and its industry partners should leverage that methodology to create a "section 9+" list, tailored to fulfill FPA emergency order requirements. Other government initiatives to prioritize critical infrastructure could also make valuable contributions to the list and overall prioritization effort. For example, DHS's May 2018 cyber strategy emphasizes the importance of "identifying the most critical [federal] systems and prioritizing protections around those systems."[184] A number of other initiatives could provide significant value as well.[185] Building a section 9+ list would also benefit from the inclusion of input from cleared state regulators and homeland security and emergency management officials.

DHS's National Risk Management Center can help integrate these sources of data and develop a comprehensive, cross-sector basis for prioritizing the sustainment and restoration of power to critical facilities. Government agencies within the center will collaborate with the private sector to "identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security." One immediate task will be to "help define what is truly critical."[186] As this work

182 Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*.

183 For methodologies and data-gathering strategies to assess cross-sector interdependencies, see EIS Council, *E-PRO Handbook III*; and Homeland Security Advisory Council, *Final Report*.

184 DHS, *Cybersecurity Strategy*, 8.

185 There are numerous programs that DOE and its partners could leverage to build the section 9+ list. DHS's National Critical Infrastructure Prioritization Program aims to identify "nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance." See DHS, *NIPP 2013*, 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on "lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity" (p. 24). Despite its focus on terrorist threats, *Homeland Security Presidential Directive 7* also requires the secretary of homeland security to identify and prioritize systems and assets that, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the "loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States" and lower jurisdictions. The national-level priorities on this list could also be helpful. 6 U.S.C. § 124l, (a)(2).

186 "National Risk Management Center Fact Sheet," DHS.

goes forward, the center's efforts could contribute to the development of a section 9+ list that will be essential for grid security emergency preparedness.

Sharing the Section 9+ List and Protecting Critical Electric Infrastructure Information

In addition to identifying assets most in need of power, it will also be essential to share that data with the utilities responsible for providing prioritized service. Current section 9 guidance lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the federal government tells grid owners and operators if they are on the section 9 list, it rarely informs them about the section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own system configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with government partners. Public sector leaders will need to reinforce their industry counterparts' confidence that government agencies will not use company-provided information for regulatory compliance, antitrust, or other purposes not explicitly approved though industry–government dialogue.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that critical companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations or supply chains in one industry can produce unintended and unforeseen effects on overall system resilience. Private companies will need to help government agencies modify the section 9+ list as they reconfigure their operations and create new dependencies on outside service and product providers.

Securing and limiting the distribution of this classified data will also be a prerequisite for countering potential attacks. If adversaries acquired the section 9+ list, it would provide a roadmap that they could use to maximize their devastation of US critical infrastructure. However, measures to protect this data must be complemented by improved mechanisms to provide sensitive information to industry personnel who have the requisite security clearances.

Section 215A of the FPA offers a starting point to meet these requirements. The FPA provides for the sharing of critical electric infrastructure information, defined as information generated by FERC or other federal agencies related to identified (or proposed) critical electric infrastructure "that is designated as critical electric infrastructure information by the Commission or the Secretary" or that qualifies under FERC's critical energy infrastructure information scheme.[187] The FAST Act amendments directed FERC to facilitate the voluntary sharing of such information "with, between, and by" BPS entities and their government partners.[188] The amendments also require FERC to create criteria and procedures to designate certain information as critical and prohibit unauthorized disclosure of that information.[189] To help meet these requirements, FERC incorporated and is building on its well-established mechanisms to protect critical energy infrastructure information.[190]

187 The definition excludes classified national security information. 16 U.S.C. § 824o–1, (a)(3).

188 This includes NERC, the E-ISAC, regional entities, and "other entities determined appropriate by the Commission." See 16 U.S.C. § 824o–1, (d)(2)(D).

189 16 U.S.C. § 824o–1, (d)(2).

190 FERC, *Regulations Implementing FAST Act Section 61003* (Order No. 833), 157 FERC ¶ 61,123, 13. See also FERC,

Other initiatives are also under way to provide for the protected data sharing essential for preplanning grid security emergency operations. DOE is working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate assets identified as defense critical electric infrastructure. Going forward, DOE, FERC, and their industry partners should refine their equivalent mechanisms to securely distribute data on critical electric infrastructure and the water systems, communications centers, and other essential non-defense assets that must continue to function in grid security emergencies.

Communications Requirements for Issuing and Employing Emergency Orders

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phones and other normal means of communication fail. These systems often provide connectivity with neighboring BPS entities and, to an increasing extent, entities that are farther away. Under the ESCC, industry has also built an extensive set of playbooks to help companies decide what to tell customers about an incident and to unify messaging between government officials and industry representatives on estimated times of restoration and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. Preparedness for grid security emergencies will require additional progress in four areas: (1) refining consultative mechanisms and protocols for the sequential (though potentially overlapping) phases of such emergencies; (2) ensuring that communications systems can survive adversaries' attacks; (3) authenticating emergency orders and protecting the security of sensitive data; and (4) determining what to say to the US public and accounting for the risk that adversaries will conduct information warfare operations to intensify panic and incite disorder.

Initial Consultations and Sustained Communications

As with the phases of grid security emergency declarations, the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Preattack consultations constitute the initial stage. As noted above, the FPA specifies that before the secretary issues emergency orders, DOE will consult with power companies and other BPS stakeholders "to the extent practicable . . . regarding implementation of such emergency measures."[191] This report recommends that federal officials also consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The grid security emergency rule clarifies how DOE's Office of Electricity Delivery and Energy Reliability will consult on emergency orders.[192] The rule states that, if practicable, the E-ISAC is one of the organizations the secretary will consult. Such consultations will be particularly useful for sharing data (including classified data) on attacks that are imminent or under way. The rule also notes that DOE will consult with the ESCC. The ESCC will provide an especially valuable source of industry perspectives on grid security emergency declarations and emergency orders because it represents all components of the electricity subsector and has extensive experience in coordinating the industry's incident response operations. In addition, the rule states that "efforts

Regulations Implementing FAST Act Section 61003 (Order No. 833-A), 163 FERC ¶ 61,125; and 18 CFR 388.113.

191 DOE, "RIN 1901–AB40," 1774.

192 DOE, "RIN 1901–AB40," 1181.

will be made" to consult with NERC, regional entities, "owners, users, or operators" of critical and defense critical electric infrastructure (including regional transmission operators), appropriate federal and state agencies, and other grid reliability stakeholders.

Issuing emergency orders constitutes the second stage. DOE's grid security emergency rule states that the department will "communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances."[193] The E-ISAC will likely play a critical role in such communications, since it maintains a detailed, continuously updated list of all BPS owners, operators, and registered users (distribution entities). DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.[194] As long as these mechanisms can be hardened as necessary to survive adversaries' attacks, leveraging them for grid security emergencies will be much more efficient than creating a separate, unfamiliar system for communicating emergency orders.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders. Attacks on the grid are unlikely to be "one and done." As adversaries continue to try to destabilize the grid, and power companies respond with emergency operations to protect and restore electric system reliability, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional orders and response activities—potentially on a nationwide basis.

Reliability coordinators will be a critical touchpoint between DOE and individual BPS entities, serving as a focal point between DOE (and other government leaders) and the power companies that are in their purview. This positioning makes them well suited to communicate secretary-issued orders to individual utilities. Moreover, given reliability coordinators' responsibilities and authorities to help maintain grid reliability when incidents occur, they will also be ideally positioned to understand how grid security emergency orders should supplement BPS emergency operations that are already under way.

Sustained communications will also be necessary to meet an additional FPA requirement: responding to DOE requests for information on the implementation of emergency orders. The grid security emergency rule specifies that "beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order."[195] Sustained communications links between DOE and BPS entities will be required to meet such requests for information. However, beyond compliance issues, continuous communications will also be required as government and industry partners assess the effectiveness of emergency operations and identify requirements for additional actions.

Survivability of Communications

Adversaries will have compelling incentives to combine attacks on the grid with strikes against US communications systems. The 2015 attack on Ukraine's electric grid illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone networks; the latter attack prevented customers from reporting outages and disrupted grid operators' ability to conduct restoration operations.[196] In turn, if adversaries can lengthen power outages by disrupting communications systems essential

193 DOE, "RIN 1901–AB40," 1181.

194 DOE, "RIN 1901–AB40," 1177.

195 DOE, "RIN 1901–AB40," 1182.

196 "Alert (IR-ALERT-H-16-056-01)."

for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications-system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually reinforcing disruptions in both sectors.

We should assume that adversaries will design their attacks to maximize multisector failures, especially since they would already be facing the risk of US response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry–government coordination in grid security emergencies. Enemies might strike communications systems to hobble efforts to share preattack threat data and convey emergency orders. Once attacks on the grid were under way, adversaries could also seek to cripple the communications systems needed to coordinate emergency operations and assess requirements for additional measures.

Strengthening the survivability of existing communications links will be essential to manage these risks. To date, ESCC consultation and coordination mechanisms have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to distributed denial-of-service attacks and a range of other increasingly severe threats,[197] as well to the loss of the grid-provided electricity on which many such systems depend (especially in long-duration outages that put emergency power assets at risk).

Adversaries may also seek to disrupt systems essential for information sharing. For example, the Cybersecurity Risk Information Sharing Program and other E-ISAC notification procedures and portals are in place to alert utilities when adversaries are implanting malware on critical systems.[198] This includes the E-ISAC's new Critical Broadcast Program, which is intended to operationalize the organization's information sharing capabilities.[199] The FBI and DHS also issue alerts to the energy sector, as in the case of CrashOverride.[200] However, many of these warning and information sharing mechanisms rely on the internet or other potentially vulnerable systems. Industry and government should explore options to ensure that they can still convey essential data in the face of sophisticated attacks on the communications sector.

In addition, adversaries may seek to disrupt the issuance of emergency orders. DOE's grid security emergency rule notes that the department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect BPS reliability, which require recipients to respond as defined in the alert.[201] DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across registered entities. NERC already distributes alerts broadly to BPS users, owners, and operators in North America. Hence, the alert system provides DOE with an opportunity for "one-stop shopping" when issuing emergency orders. The secretary could issue an order to NERC for distribution to both regional operating organizations (regional transmission organizations, independent

[197] Banham, "DDoS Attacks."

[198] "Energy Sector Cybersecurity Preparedness," DOE; and "Electricity Information Sharing and Analysis Center," NERC.

[199] The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See Lawrence, de Seibert, and Daigle, "E-ISAC Update."

[200] "Alert (TA17-163A)."

[201] "About Alerts," NERC.

system operators, reliability coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is email based.[202] As such, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also includes only those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for implementing emergency orders for prioritized load shedding and other actions to sustain power to critical facilities.

Moreover, while the NERC alert system could provide a means of communications across BPS users, owners, and operators, NERC primarily uses the system to communicate alerts of voluntary actions to be taken by electric industry stakeholders. Using the NERC alert system to instead communicate a mandatory action pursuant to a DOE emergency order would require clear coordination and communication to ensure that the order and associated requirements for action are fully understood. In addition, while the NERC alert system offers a proven means to convey unclassified information, the system may not be well suited to distribute classified data.

To fill these gaps, industry and government partners should consider measures to bolster the NERC alert system or create fallback options for survivable communications. Satellite phones offer a prominent option for operational coordination. These phones are widely deployed both among BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies.

[202] "About Alerts," NERC.

Retired US Air Force General William Shelton, who directed the US Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community."[203]

Accordingly, power companies are ramping up their investments in terrestrial emergency communications systems that are hardened against cyber and physical attacks and can be used to sustain critical grid functions even if satellite phones fail.[204] Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are under way to build dark fiber or other survivable links between BPS entities—much less between those entities and DOE. The National Infrastructure Advisory Council study *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system traffic and reserved spectrum for backup communications during emergencies."[205]

The council's study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. In doing so, DOE should leverage lessons learned from the communications sector and specifically from the National

[203] Shelton, "Threats to Space Assets," 3.

[204] FERC and NERC, *PRASE*, 15.

[205] NIAC, *Securing Cyber Assets*, 7.

Security Telecommunications Advisory Committee, which has extensive experience in building redundant and survivable systems.[206] However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities "can communicate with utility crews working in the field to manually restore power" and conduct other postattack operations.[207] Survivable communications systems must also be able to coordinate emergency operations across the electricity subsector and with supporting government agencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when those orders are needed most.

Authenticating and Securing Emergency Orders

In addition to disrupting the availability of communications systems, adversaries may also seek to corrupt the content of emergency orders and coordination messages, and gain access to classified US data to help defeat grid protection measures. One near-term requirement will be to ensure that utilities can authenticate the orders they receive from DOE. Power companies will need to be able to verify that an order has actually come from the secretary, and that adversaries have not altered its content. Verifying the authenticity of orders will be especially important if such orders require extraordinary measures that could further disrupt normal service and affect public health and safety.

Existing mechanisms and protocols to ensure the integrity of subsector communications provide an initial basis to meet these challenges. Other government agencies have also developed authentication protocols that could be adapted for use in grid security emergencies. For example, the *DoD Cybersecurity Discipline Implementation Plan* (February 2016) offers detailed guidance to strengthen authentication in the face of adversary efforts to exploit communications networks and devices.[208]

Adversaries may also seek to gain access to classified or operationally sensitive emergency orders. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as possible, lest those operations create incentives for adversaries to strike before their advanced persistent threats were disabled. When attacks are under way, it could be useful to deny adversaries the knowledge of where and how BPS entities are prioritizing the flow of power to vital military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important, given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The FPA and subsequent grid security emergency rule provide for the sharing of classified information in grid security emergencies. The rule specifies that:

> To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.[209]

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program already have mechanisms and protocols for sharing and securing classified threat

206 "About NSTAC," DHS.

207 NIAC, *Securing Cyber Assets*, 7.

208 DOD, *DoD Cybersecurity Discipline Implementation Plan*.

209 DOE, "RIN 1901–AB40," 1182.

data with BPS entities cleared for access to that data.[210] Industry and government partners should consider building on those mechanisms to support the issuance of classified emergency orders. Ongoing progress under the Cybersecurity Risk Information Sharing Program will be valuable as it serves a growing array of utilities, accesses additional sources of data and advanced analytic tools, and continues other improvements.

DOE and its partners in industry and government might consider sharing this classified data in other ways. For example, DHS and other federal partners such as the FBI and the National Guard have secure video teleconference capabilities. However, these are technologically complex and not seamlessly interoperable with industry systems. Moreover, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Section 215A addresses this issue by ordering the secretary to "facilitate and, to the extent practicable, expedite," the security clearance process for key personnel of any entity subject to emergency orders to enable "optimum communication" of threat information.[211] DOE should accelerate its ongoing efforts to meet this requirement. The section also grants the secretary and other appropriate federal agencies the authority to provide temporary access to classified information regarding grid security emergencies and subsequent orders to key personnel of complying entities.[212]

Yet, even for utilities with cleared personnel on their staffs, an even smaller number possess the sensitive compartmented information facilities or other infrastructure and government approvals to store classified information. To address those limitations, the grid security emergency rule clarifies that the secretary may declassify information critical to the emergency response.[213] But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of combatant commander operational plans; when emergency orders may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

Communicating with the American People

Adversaries may attack the grid not only to disrupt national defense and the economy but also to gain political leverage over US leaders by inciting public panic and disorder. A presidential declaration that the grid faces imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the US public.

Preplanning for public messaging to accompany grid security emergency declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges in such events. However, those difficulties will be dwarfed by the problems that adversaries can create through cyber attacks. Attackers may:

- Use information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety
- Intensify state and local requests for defense support to civil authorities to deal with these

[210] "Energy Sector Cybersecurity Preparedness," DOE.

[211] 16 U.S.C. § 824o–1, (e).

[212] 16 U.S.C. § 824o–1, (b)(7).

[213] DOE, "RIN 1901–AB40," 1778.

anticipated effects, and thereby put pressure on US leaders to divert scarce defense assets and resources from other missions

- Disrupt normal means of communication on which the public will rely for information about the event
- Magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats that enable repeated reattacks and disruptions in grid service until eradicated from BPS networks.

DHS's Social Media Working Group for Emergency Services and Disaster Management has offered preliminary recommendations on how to counter disinformation during disaster response operations.[214] In addition, the ESCC and its members are developing playbooks to help meet disinformation challenges and support public messaging in the event of cyber or physical attacks against the grid.[215] Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that presidential grid security emergency declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Preplanning for message coordination with Canada and Mexico could also be helpful and might leverage the FPA's provisions for such multinational consultations concerning the issuance of emergency orders.[216]

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. For example, some orders that will be valuable for protecting grid reliability, including those for prioritized load shedding, could cut off electricity to many thousands of customers to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

The Deeper Value Proposition for Emergency Orders: Political Top Cover, Waivers, and Cost Recovery

The grid security emergency provisions of the FPA do not even mention a significant advantage that orders can provide for industry: they can help protect power companies from the political heat that extraordinary grid protection measures will create. The FPA's provisions for regulatory waivers and cost recovery offer more explicit benefits. Yet, given the risks that utilities could incur in conducting emergency operations, and the investments in infrastructure that may be required to facilitate order implementation, Congress and DOE should consider additional measures to help power companies defend the grid and protect national security.

Facilitating Operations under Extraordinary Political Circumstances

In responding to natural hazards, power companies can fall under intense pressure to serve the priorities of state and local elected officials. In severe weather events, for example, governors have told utilities to delay sending restoration resources to assist neighboring states until service has been restored to *all* customers (i.e., voters) in the governors' own states.

Cyber and physical attacks on the grid could create still more intense political pressure, and complicate utilities' efforts to serve national priorities versus those most urgent to meet state and local needs. Such attacks will occur in the context of broader risks of all-out war and will magnify public fears in ways that hurricanes or other natural hazards cannot—especially if those attacks are accompanied by

[214] Social Media Working Group for Emergency Services and Disaster Management, *Countering False Information*.

[215] ESCC, "ESCC: Electricity Subsector Coordinating Council."

[216] 16 U.S.C. § 824o–1, (b)(3).

information warfare operations to incite public panic. Governors will have powerful incentives to ensure that utilities in their states take care of their own citizens rather than meeting requests for assistance from power companies in other states.

However, from a national security perspective, not all states and customers within them will be of equal importance for protecting defense critical electric infrastructure. Some low-population states served by utilities with only limited resources are the homes of vital military installations. These utilities may need assistance from out-of-state power companies to supplement their own personnel and response capabilities when adversaries strike.

The electric industry's Cyber Mutual Assistance (CMA) Program will be critical for providing such support.[217] DOE is expanding the technical resources and capabilities available to support CMA response operations.[218] Under the national response event initiative, investor-owned utilities (led by the Edison Electric Institute) are also bolstering mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States.[219] All of these initiatives will be vital for responding to grid security emergencies that entail multiregional disruptions of the BPS or degrade critical electric infrastructure that the infrastructure's owners cannot restore on their own.

Yet, the voluntary nature of these mutual assistance systems could present challenges in grid security emergencies. In hurricanes or other natural hazards, governors and utilities can predict whether or not their states are likely to be struck and either husband their resources accordingly or provide them in response to requests for assistance. Cyber and physical attacks by Russia, China, or other potential adversaries are much less predictable. Enemies may strike one region before moving on to others. Attacks could even occur on a nationwide basis. Accordingly, elected officials may discourage utility leaders from volunteering resources for mutual assistance in neighboring regions, even if their own states have not yet been struck.

Issuing emergency orders can help utilities address these challenges and serve national priorities. Participants in the Cyber Mutual Assistance Program are already taking steps to account for the risk of multiregional attacks. DOE and its industry partners should preplan to reinforce those measures in grid security emergencies. If the secretary orders utilities to help protect or restore grid reliability beyond their service areas, those orders will help justify (and indeed, legally require) providing such assistance, regardless of the political pressure against doing so. DOE should consider reaching out to state and local leaders and their senior energy appointees before emergencies occur in order to ensure that they are familiar with the FPA requirements and the national security value of mutual assistance.

Emergency orders can also help utilities execute politically unpopular emergency operational decisions within their own service areas. Cyber and physical attacks could put utility CEOs in the unenviable position of having to manage shortfalls in available power by depriving lower-priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The secretary of energy can give CEOs political top cover for taking such unpopular actions, rather than leave them to act on a voluntary basis and bear the full brunt of explaining why they did so.

Exercises can help utilities and government officials prepare to collaborate in the face of intense political pressures, and coordinate the execution of emergency orders on a nationwide basis. NERC already requires BPS entities to exercise their individual emergency and power system restoration plans. In the GridEx exercise series, over one hundred utilities across the

217 ESCC, "Cyber Mutual Assistance Program."

218 DOE, *Multiyear Plan*, 29.

219 EEI, *Understanding the Electric Power Industry's Response and Restoration Process*.

United States and Canada test the use of their plans against combined cyber-physical attacks and exercise the use of Cyber Mutual Assistance protocols and procedures. Building template emergency orders and utility-specific implementation plans will provide an even stronger basis for coordinated multientity exercises. In planning for GridEx V in 2019, NERC and its government and industry partners should consider the possibility of exercising the issuance and implementation of specific template emergency orders. State, local, tribal, and territorial participation in utility exercises that include the use of emergency orders will also be crucial.

Environmental, Regulatory, and Legal Waivers

In amending the FPA to address grid security emergencies, Congress provided power companies with an important protection for complying with emergency orders—one that they might not receive by implementing equivalent emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate FERC-approved grid reliability standards or other rules or provisions under the FPA, the act specifies that those actions "shall not be considered a violation" of those provisions. Such waivers of enforcement apply unless a complying entity acts in a "grossly negligent manner."[220]

The FAST Act amendments to the FPA also introduced broader protections into section 202(c), absolving entities from violations of federal, state, or local environmental laws or regulations that occur as a result of complying with an order. That provision shields complying entities from "any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation."[221] These protections apply to section 215A emergency orders as well.[222]

FPA-based waivers will be especially valuable for certain types of emergency orders. For example, if the secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service, such as proactively shedding firm load, could also violate NERC's FERC-approved reliability standards.[223] Separating preplanned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards as well.

The waiver process under the FPA is structured to function automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that a BPS entity has acted with gross negligence. Nevertheless, industry, DOE, and regulators might find it useful to build consensus on the types of waivers that specific template orders should include.

Their discussions could also help address more far-reaching regulatory issues that grid security emergencies may pose. For example, the FPA does not provide waivers for Nuclear Regulatory Commission regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the commission would enforce a violation of its regulations by a nuclear generation entity complying with an emergency order. The worst time to adjudicate such a dispute, however, would be in the midst of a grid security emergency. Pre-event discussions will be particularly important given the nuclear fleet's imperative to protect public health and safety. DOE, the Nuclear Regulatory Commission, and their industry partners will need to ensure that assessments of regulatory issues associated with

220 16 U.S.C. § 824o–1, (f)(4).

221 16 U.S.C. § 824a, (c)(3).

222 16 U.S.C. § 824o–1, (f)(2).

223 For example, in events such as the September 2011 Arizona–California disturbance, FERC has found that load shedding led to violations of NERC's reliability standards.

emergency operations take safety considerations into full account.

Preplanning will also be vital for emergency orders that support power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that "the storage of strategically located spare large power transformers" and other critical grid components "will reduce the vulnerability of the United States to multiple risks facing electric grid reliability," including cyber and physical attacks.[224] Accordingly, Congress required DOE to develop a strategic transformer reserve plan to determine the number and type of spare large power transformers that should be stored and to examine issues associated with transporting those spares.[225]

DOE responded to this requirement by providing a strategic transformer reserve report (March 2017). The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a more substantial pool of spare large power transformers than DOE had anticipated and that a federally owned reserve is not needed.[226] However, the plan also found that it was crucial to ensure that large power transformers can be efficiently moved during national emergencies.[227]

Regulatory waivers can play a critical role in facilitating that movement. The higher-voltage classes of large power transformers, including 765-kilovolt transformers, are as big as a house and can be moved—slowly and very carefully—only by specialized heavy-haul trucks, railcars, and barges. Under the auspices of the ESCC, utilities have established the Transformer Transportation Working Group to analyze the problems posed by moving large power transformers in an emergency and to build collaborative plans with transportation companies and associations. A central finding of the group's analysis: regulatory waivers will be critical to expedite the movement of large power transformers, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.[228]

DOE's 2017 transformer report committed the department to coordinating with the Transformer Transportation Working Group "to improve and optimize transportation planning in response to a significant national event impacting the electricity grid."[229] However, the report did not examine how emergency orders and implementation plans might speed the transportation of large power transformers. As DOE collaborates with the working group and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols that are not addressed by the FPA and that pose the greatest impediments to transformer movement. DOE and its partners should then preplan to waive these provisions if the secretary issues emergency orders.

The challenge for such preplanning: the secretary of energy lacks the statutory authority to waive key transportation regulations. Most federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of DOT. Federal regulations and emergency operations that would govern the movement of transformers on barges, which could be critical for restoring power for coastal cities and along the Mississippi–Ohio river system of inland waterways, are overseen by the US Coast Guard and the US Army Corps of Engineers. State and local transportation regulations and permitting requirements will also

224 FAST Act, 1779.

225 FAST Act, 1780–1782.

226 DOE, *Strategic Transformer Reserve*, 21.

227 DOE, *Strategic Transformer Reserve*, 1.

228 ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies*, 22–23.

229 DOE, *Strategic Transformer Reserve*, 22.

pose major impediments to moving large power transformers over roads unless adequate waivers are in place to lift restrictions.

DOE should build collaborative plans to employ waiver authorities beyond those directly under the secretary's control. For example, to facilitate the movement of large power transformers, gubernatorial disaster declarations could help waive state-level regulations. The American Association of State Highway and Transportation Officials and National Emergency Management Association are exploring the use of these and other waiver authorities. DOE is also preplanning with other federal, state, local, tribal, and territorial agencies to coordinate response operations under Emergency Support Function #12—Energy.[230] Especially valuable, a growing number of individual power companies are creating contingency plans for emergency transportation with government agencies and road, rail, and barge companies. Building on these efforts, and on initiatives led by the Transformer Transportation Working Group,[231] the electricity subsector and its partners should establish systematic, nationwide plans to facilitate the movement of transformers and other critical equipment in grid security emergencies.

Over the longer term, Congress, industry, and government partners should also consider whether complying entities should have liability protections beyond those currently provided by the FPA. Prioritized load shedding for extended periods will create "winners and losers" in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other section 9+ assets may leave shortfalls in electric service at dialysis centers, small urgent-care centers, and facilities for special-needs citizens. These disruptions will put lives at risk. Legislators, DOE, and electric industry leaders should examine whether utilities complying with such necessary but highly disruptive emergency orders ought to have additional liability protections. Cutting off power to lower-priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.[232] Again, if these risks of exposure are sufficiently severe, Congress should consider providing further protections for BPS entities.

Cost Recovery for Emergency Operations and Support for Investments in Grid Infrastructure

Complying with emergency orders may force utilities to incur costs beyond their normal operating expenses. The FPA states that if FERC determines "that owners, operators, or users of critical electric infrastructure have incurred substantial costs" in complying with an emergency order, FERC shall "establish a mechanism that permits such owners, operators, or users to recover such costs."[233] Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other orders could require reimbursement through FERC-directed mechanisms as well.

The act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that emergency orders require utilities responsible for defense critical electric infrastructure to take emergency measures, the "owners or operators" of critical defense facilities that rely on such infrastructure "shall bear the full incremental costs of the measures."[234] Fair warning to DOD: it

[230] "State and Local Energy Assurance Planning," DOE.

[231] DOE, *Strategic Transformer Reserve*, 12.

[232] Frankel, "Can Customers Sue Power Companies for Outages?"

[233] The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs "prudently" and that those costs "cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users." 16 U.S.C. § 824o–1, (b)(6)(A).

[234] 16 U.S.C. § 824o–1, (b)(6)(B).

should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- attacks create major blackouts and deprive utilities of revenue;
- emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- adversaries disrupt financial markets, either through direct cyber attacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.[235]

Power companies are strengthening their plans and capabilities for cross-sector support with the financial services sector.[236] These efforts should include the development of contingency plans for financial-services companies (in coordination with the Department of Treasury and DOE) to help utilities cover the urgent expenses they may incur in responding to grid security emergencies. In addition, to facilitate the reimbursement process provided for in the FPA, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with orders will be more difficult once attacks are under way.

Cost recovery for investments in grid infrastructure to facilitate emergency order implementation will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. Other orders may be impossible to execute unless BPS entities make additional investments in infrastructure. It will be near useless to order transmission operators to protect or rapidly restore service to vital but remote military bases served by a single transmission line if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure that these facilities can help defeat US adversaries when the nation is under attack. DOD will need to develop a cost-recovery mechanism to reimburse defense critical electric infrastructure owners for making such investments.

To be even remotely viable as an emergency order design option, most preplanned power islands will also require at least some infrastructure construction. Ideally, these preplanned islands will use existing generation, transmission, and distribution assets within their service footprints to separate from the grid and still be able to provide reliable electric service to the section 9+ assets insider their borders. But many areas that might be designed to function as islands in a grid security emergency will lack adequate infrastructure to do so. The grid's interconnected design enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Preplanned power islands will not only lose those reliability benefits, but they will also have to make do with infrastructure that utilities built and aligned to be supporting components of the interconnected grid—*not* self-sustaining islands that would be stood up in grid security emergencies. Moreover, operating and recovering from preplanned island schemes will create an entirely different operating mode than industry is currently designed

[235] NERC, *GridEx III Report*, 15.

[236] See, for example, the Strategic Infrastructure Coordinating Council (SICC). ESCC, "ESCC: Electricity Subsector Coordinating Council."

for. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: to be effectively implemented, many emergency orders could require spending on new transmission lines and other grid infrastructure.

The FPA provisions for grid security emergencies do not explicitly authorize reimbursement for infrastructure investments. While the act requires FERC to establish a mechanism to enable owners, users, and operators of critical and defense critical electric infrastructure to recover their costs of complying with emergency orders, those funding provisions do not mention preattack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover costs for infrastructure investments in resilience against cyber and physical attacks.[237] FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate emergency order execution.

Similar discussions will be necessary with state public utility commissions. As noted above, local distribution systems will play vital roles in implementing emergency orders. Public utility commissions have primary regulatory authority over such distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. They could also make important contributions to reviewing proposed implementation plans for emergency orders that would be executed within their respective states, particularly when local distribution systems would be necessary to implement the orders.

The FPA opens the door to such discussions. The act states that FERC and the secretary of energy "shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions."[238] Initiating these discussions with the National Association of Regulatory Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has extensively analyzed criteria for assessing the prudence of investments against cyber and physical attacks and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

Conclusions and Recommendations for Broader Progress

Taken together, the options for industry–government collaboration examined in this report constitute a massive undertaking for which Congress appropriated zero funding to utilities. Developing a sequenced, prioritized strategy to explore these options will help make doing so a more manageable task.

Potential emergency orders will differ not only in terms of the phases of an attack in which they would be most useful, and in the degree to which they will disrupt normal electric service, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create—especially those that fall into the no-regrets category. Utilities frequently use conservative operations to help protect grid reliability in severe weather events. A growing number of companies are

[237] See, for example, FERC, *Extraordinary Expenditures* (96 FERC ¶ 61,299), 1; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), 10–11; and FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), 60.

[238] 16 U.S.C. § 824o–1, (d)(4).

already building on that foundation to draft equivalent conservative operations against cyber and physical threats. Emergency orders based on these initiatives constitute "low-hanging fruit"; creating such orders offers an immediate opportunity for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging emergency order initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are under way, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. Improving communications survivability and preplanning to counter disinformation campaigns will also be crucial for grid security emergency preparedness. So, too, will be efforts not only to fully leverage the FPA's regulatory waiver and cost recovery mechanisms but also to explore additional liability protections and other measures to help entities comply with emergency orders.

A comprehensive plan to align and integrate these initiatives should also address three additional opportunities to build resilience for grid security emergencies: (1) preplanning to use additional federal and state emergency authorities to defend natural gas systems, communications networks, and other infrastructure on which the grid depends; (2) coordinating with Canada, Mexico, and other nations whose grids may be struck in conjunction with attacks on US electric systems; and (3) exploring new options to deter and defeat attacks on the grid by integrating defensive measures with government operations to blunt further strikes on US power companies and other targets.

Employing Additional Emergency Authorities for Cross-Sector Resilience

Building preparedness against attacks on the grid is necessary but not sufficient to protect BPS reliability. In many US regions, power generation is becoming extraordinarily dependent on the flow of natural gas. Adversaries may attempt to cause cascading blackouts and other major grid instabilities by crippling natural gas systems. To hedge against such disruptions, some generators have the ability to operate on diesel and other secondary fuels if attackers interrupt gas supplies. But the refining and transportation systems needed to resupply such "dual-fuel" generators with diesel will themselves be at risk in grid security emergencies.[239] Moreover, as examined earlier in this report, coordinated grid restoration will also depend on the availability of communications systems and other infrastructure sectors.

This report has focused on employing the emergency authorities that Congress incorporated into the FPA by creating section 215A of the act in 2015. However, these authorities apply only to BPS owners and operators. The secretary cannot issue emergency orders under 215A to operators of natural gas and diesel fuel systems, much less to telecommunications companies and other infrastructure owners beyond the energy sector. The secretary has a range of other emergency authorities, including the Defense Production Act (DPA) and the authorities provided by section 202(c) of the FPA, which could facilitate coordinated response and restoration operations across the energy sector. The analysis that follows examines how DOE and its industry partners could preplan for the integrated use of all such authorities in a grid security emergency. This analysis also examines how federal and state leaders might use additional emergency powers to coordinate multisector response operations.

[239] The author has advised Exelon Corporation on risks of fuel interruptions for power generation. Exelon has provided no funding for this report.

Coordinating Emergency Operations among Electric Utilities, Natural Gas Systems, and Other Energy Sector Components

Natural gas is an increasingly important source of fuel for power generation in many regions of the United States. Between 2002 and 2016, the nationwide share of electricity provided by gas-fired units increased from 18 percent to approximately 34 percent.[240] However, in New England, California, and other parts of the United States, natural gas has become the predominant source of fuel for power generation.

ISO New England has highlighted the risks that this reliance creates for grid resilience. It notes that "in New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability."[241]

Other regions also face growing fuel supply risks to grid resilience. A DOE-sponsored report titled *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units, Volume I: The Critical Role of Thermal Units During Extreme Weather Events* (March 2018) notes that many regional transmission organizations and independent system operators will face a combined challenge of inadequate natural gas pipeline infrastructure and competing demands for fuel from users apart from power generators.[242] More broadly, NERC has found that "the electric sector's growing reliance on natural gas raises concerns regarding the ability to maintain BPS reliability when facing constraints on the natural gas delivery systems."[243] NERC's *2016 Long-Term Reliability Assessment* also notes that "as part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability."[244] Additionally, in *Grid Resilience in RTOs and ISOs* (January 2018), FERC called for additional data to better assess the risks posed by "wide-scale disruption to fuel supply" that could result in outages of multiple generators.[245]

Companies in the oil and natural gas subsector are bolstering their capabilities to protect their critical system components from attack and are taking new measures to ensure the continued safe and reliable delivery of natural gas to critical customers, including power generators.[246] However, threats to the oil and natural gas subsector are rapidly escalating as well.[247] As gas system owners and operators address these increasing threats, new opportunities will emerge for joint gas–electric resilience initiatives and emergency planning.

The oil and natural gas and electricity subsectors are already improving their coordination on resilience issues.[248] Moreover, NERC has been facilitating coordination between BPS entities and natural gas companies to address fuel resilience and interdependency challenges.[249] The ESCC has also been developing new coordination mechanisms for the

240 DOE, *Staff Report to Secretary*, 90.

241 ISO-NE, "Response of ISO New England Inc.," 1.

242 NETL, *Reliability, Resilience and the Oncoming Wave*, 4, 14, 22, 3.

243 NERC, *Short-Term Special Assessment*, 12. See also NERC, *2013 Special Reliability Assessment*.

244 NERC, *2016 Long-Term Reliability Assessment*, 21.

245 FERC, *Grid Resilience*, 161 FERC ¶ 61,012 (2018), 14. See also Stockton, *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*.

246 "Cybersecurity," American Gas Association.

247 Sobczak, Northey, and Behr, "Cyber Raises Threat"; and Stockton (on behalf of Exelon Corporation), *Prepared Direct Testimony* (Docket No. RM18-1-000), 13.

248 DOE, *Staff Report to Secretary*, 94; and EIS Council, *E-PRO Handbook II*, 189.

249 NERC, *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*, 1.

two industries (as well as with communications and financial services sectors).[250] Additionally, the natural gas industry participated in GridEx IV, which examined opportunities to mitigate the risk that adversaries will simultaneously attack gas and electric systems.

Building on these and other collaborative efforts, gas and electric companies (and their regulatory partners) should examine how they can prioritize support for each other in grid security emergencies. For example, when blackouts occur, electric companies typically prioritize the restoration of service to compression stations and other electricity-dependent gas infrastructure that is essential to supply fuel for power generation and other critical customers. Support for gas infrastructure should remain a priority, even as BPS entities add other section 9+ facilities to their restoration plans. Gas companies might also reassess their curtailment policies to help gas-dependent BPS entities sustain service to major military installations and other vital facilities in grid security emergencies.[251]

BPS entities and DOE should also pursue deeper collaboration with the companies that refine and deliver secondary fuels for power generation. If adversaries interrupt the flow of natural gas, dual-fuel generators can use diesel, no. 2 fuel oil, or other secondary fuels to sustain their operations in a grid security emergency.[252] However, cascading blackouts could disrupt the flow of these secondary fuels as well. Refining and transportation systems components that are essential to resupply dual-fuel generators depend on electricity. Adversaries may also attack these systems at the same time they strike the grid. Moreover, ongoing cutbacks in industry delivery capacity could magnify these risks of interruption. ISO New England notes that a "withering delivery supply chain" constitutes an "unquantifiable X factor" in assessing grid resilience.[253] Preplanning to prioritize the delivery of secondary fuels for power generation will be essential for grid security emergencies, especially given the enormous demand for diesel from emergency power generators from hospitals, water utilities, and other vital facilities in wide-area blackouts.

Emergency authorities beyond 215A can help prioritize the flow of natural gas and secondary fuels to protect and restore grid reliability. The DPA will be especially helpful in this regard. The act is the "primary source of presidential authority to expedite and expand the supply of critical resources from the U.S. industrial base to support the national defense and homeland security."[254] The DPA defines national defense to include "critical infrastructure protection and restoration," encompassing all electric system components and supporting fuel supply infrastructure (including natural gas pipelines) that are at risk of cyber and physical attacks.[255] In 2012, the White House delegated many of the president's DPA authorities to the heads of relevant federal agencies, including the secretary of energy for prioritization and allocation decisions regarding "all forms of energy."[256]

Especially valuable for cross-sector resilience, DOE has established an Energy Priorities and Allocations System that enables the department to prioritize contracts for the delivery of natural gas, diesel, and other energy resources between the companies that provide them and government agencies, electric utilities, and other private and public sector customers. The system also enables DOE to allocate energy materials, services, and facilities to promote

250 ESCC, "ESCC: Electricity Subsector Coordinating Council."

251 EIS Council, *E-PRO Handbook II*, 219.

252 ISO-NE, *Operational Fuel-Security Analysis*, 52; and NERC, *2013 Special Reliability Assessment*, 4.

253 ISO-NE, *Operational Fuel-Security Analysis*, 14, 16.

254 DHS, *Power Outage Incident Annex*, 129.

255 50 U.S.C. § 4552, (14).

256 Obama, *Executive Order—National Defense Resources Preparedness*.

"critical infrastructure protection and restoration" and emergency preparedness.[257]

DOE has already used its authorities under the DPA to support power generation in previous energy crises. In 2001, for example, the department used these authorities to ensure that emergency supplies of natural gas continued to flow to Californian power generators, thereby helping to avoid threatened electrical blackouts.[258] Now, to build preparedness for grid security emergencies, DOE and its industry partners should consider preplanning to use the DPA to sustain or restore gas and diesel deliveries to critical generators, including those that serve microgrids on defense installations, regional hospitals, and other assets critical for national security and public health and safety.

DOE could use the DPA to support and prioritize power restoration operations in other ways as well. Section 101(a) of the act provides DOE with the authority to prioritize the delivery of critical grid components in an emergency. If coordinated physical attacks damage or destroy transformers at a large number of critical substations, the secretary could use the DPA to allocate replacement transformers in ways that most directly benefit national security and public health and safety.

Two additional sources of emergency authorities could further strengthen preparedness and supplement the use of section 215A emergency orders. The first is section 202(c) of the FPA. The section authorizes the secretary to order "temporary connections of facilities and such generation, delivery, interchange, or transmission of electric energy as in its judgment will best meet the emergency and serve the public interest." That provision also specifies that the secretary could exercise such powers "during the continuance of any war in which the United States is engaged, or whenever the Commission determines that an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy or of facilities for the generation or transmission of electric energy, or of fuel or water for generating facilities, or other causes."[259]

A key virtue of section 202(c) is that the secretary can apply these emergency authorities to local distribution systems that might not fall within the purview of section 215A. Moreover, DOE has a strong record of having used 202(c) authorities in past emergencies, including the California Enron crisis, Hurricane Katrina, and other events.[260] DOE and its industry partners should consider building on this foundation to plan for the use of these authorities in grid security emergencies.

The Natural Gas Policy Act provides further authorities that could help coordinate energy sector operations in grid security emergencies. The president must declare a natural gas supply emergency before the secretary gains emergency powers under the act. The president can make such a declaration if there is evidence of an imminent or existing "severe natural gas shortage, endangering the supply of natural gas for high-priority uses" and that, having exhausted other alternatives "to the maximum extent practicable," natural gas emergency authorities are necessary to resolve the situation.[261] The president may also delegate this authority, as well as the authority to issue rules or orders, to the secretary of energy or other appropriate federal officials.[262]

The president or secretary can issue two main types of orders or rules. Most important, during a natural gas supply emergency, the act authorizes the president or other officials to allocate natural gas supplies "to assist in meeting natural gas requirements for high-priority

257 DOE, "RIN 1901–AB28," 33615, 33622–33626.

258 Brown and Else, *Defense Production Act of 1950*, 10.

259 16 U.S.C. § 824a, (c)(1).

260 "DOE's Use of Federal Power Act Emergency Authority," DOE.

261 15 U.S.C. § 3361, (a).

262 15 U.S.C. § 3364, (d).

uses."[263] The secretary could use this provision to ensure that critical generating facilities get the fuel they need.

Of course, some of these authorities overlap. DOE and its government and industry partners should develop an integrated approach to employing these powers for grid security emergencies, and determine which particular authorities are best suited to meet specific energy sector risks that cyber and physical attacks can create. These partners, along with other energy sector stakeholders, should also consider exercise scenarios that involve the simultaneous use of multiple emergency authorities to simulate the complex legal environment they may be faced with in a grid security emergency.

Multisector Resilience for Grid Security Emergencies

An overarching strategy for grid security emergency preparedness should also advance operational coordination between energy companies and other infrastructure sectors that both rely on electricity and play vital roles in power restoration. Additional federal emergency authorities and incident response plans can help strengthen coordination between these interdependent sectors.

Using this broader array of plans and authorities will be particularly important if adversaries simultaneously attack multiple infrastructure sectors. By striking other sectors together with the grid, adversaries can exploit interdependencies between them to maximize the attack's disruptive effects on national security, including the ability of defense installations and supporting civilian infrastructure to conduct operations abroad.[264] The *National Cyber Incident Response Plan* provides a framework for strengthening multisector coordination mechanisms for such attacks. As the administration refines the plan, DOE and its government and industry partners should ensure that the issuance and execution of emergency orders fit within this broader framework and directly contribute to multisector resilience.

Updates to the *National Response Framework* and other FEMA-led initiatives can offer further benefits for grid security emergencies. In its after-action report from the 2017 hurricane season, FEMA noted that emergency managers and their private sector partners lack the multisector coordination mechanisms necessary to accelerate the restoration of electric power and other lifeline services.[265] The report called for FEMA to build "a cross-sector approach to the Agency's planning, organizing, response, and recovery operations," and revise current national-level planning frameworks to create a cross-sector emergency support function.[266] DOE and industry should partner to prioritize support for power sustainment and restoration within this broader initiative.

The *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* provides a prime opportunity to embed cross-sector coordination efforts in regional incident response plans.[267] The annex calls for the development of regional plans to build resilience against extended multistate blackouts and ensure that interdependent sectors can accelerate power restoration while also countering threats to public health and safety.[268] In many areas of the United States, utilities are already helping DOE, FEMA, and their state and local partners build such plans for their regions. Cross-sector preparedness for grid security emergencies should become a key focus of future power outage incident planning efforts.

263 15 U.S.C. § 3363, (a).

264 Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 11.

265 FEMA, *2017 Hurricane Season FEMA After-Action Report*, 13.

266 FEMA, *2017 Hurricane Season FEMA After-Action Report*, 12–13.

267 EIS Council, *E-PRO Handbook III*, 45.

268 DHS, *Power Outage Incident Annex*, 77.

In all of these planning and operational coordination initiatives, DOE and other departments responsible for specific infrastructure sectors should examine how other federal emergency authorities might supplement those that apply to the energy sector. The communications sector provides one such opportunity. The president has extensive authorities to address national security and emergency preparedness telecommunications issues under the Communications Act, including the power to prioritize the use of communications capabilities and provide complying entities with legal and regulatory protections.[269] Executive Order 13618 assigns many of these authorities and associated responsibilities to federal departments and agencies. The secretary of commerce, for example, is responsible for developing plans and procedures for emergency use of radio frequencies and other communications systems.[270] The secretary of homeland security is responsible for overseeing the development, testing, and implementation of emergency communications capabilities.[271] Using these capabilities to support power restoration could be enormously helpful in grid security emergencies. Equivalent emergency authorities for other sectors could assist restoration as well. However, as with all such opportunities, effectively using these federal authorities will depend on extensive preplanning.

State governors are likely to invoke their own authorities to respond to grid security emergencies. Governors have primary responsibility for protecting the health and safety of their citizens. Cyber and physical attacks on the grid, especially if paired with strikes against communications systems and other interdependent sectors, could disrupt hospitals, water systems, and other assets on which their citizens rely. Governors in every state have the ability to declare emergencies and issue executive orders to help deal with such threats to public health.[272] A growing number of states are also including utility representatives in their emergency operations centers, building collaborative plans and coordination mechanisms to respond to attacks on the grid, and preparing for state National Guard personnel to help utilities defend and restore the flow of power. These initiatives are bolstering overall preparedness for grid security emergencies. However, if multiple governors employ their own emergency authorities and implement state-level blackout response plans, it will be enormously difficult to coordinate their efforts with federal actions—including the issuance of DOE emergency orders to utilities in those very same states.

The only way to overcome such difficulties is to exercise the use of all of the authorities that could help protect and restore grid reliability, across multiple sectors and with the participation of both federal and state leaders. GridEx IV offered an important step forward in this regard. Exercise participants from the oil and natural gas subsector, as well as the financial-services and communications sectors, contributed perspectives on how they could help utilities respond to cyber and physical attacks on the grid. Representatives from state governments discussed how governors might act in such an emergency. GridEx V will provide an opportunity to address such coordination challenges in greater detail. GridEx V could also exercise the use of specific template emergency orders, together with communications mechanisms and playbooks developed for grid security emergencies. Additional exercises by BPS entities and their partners at all levels of government will also be vital to prepare for the implementation of such orders.

Extended Partnership Requirements within the United States and Abroad

Congress implicitly imposed geographic constraints on the secretary's authority to issue emergency orders to protect the reliability of defense critical electric

[269] 47 U.S.C. § 606.

[270] Obama, *Executive Order—Assignment*, section 5.3.

[271] Obama, *Executive Order—Assignment*, section 5.2. See also DHS, "Emergency Communications."

[272] Orenstein and White, "Emergency Declaration Authorities."

infrastructure. The FPA limits such infrastructure to that which is located in the forty-eight contiguous states or the District of Columbia.[273] However, Alaska and Hawaii are home to vital grid-dependent military installations and supporting civilian infrastructure, including facilities for US continental ballistic missile defense and command and control of military operations in the Pacific region. Key defense installations also exist in Guam and other US territories. As the electric industry and DOE build preparedness for grid security emergencies, they should consider collaborating with the utilities that serve these states and territories and their government partners (including DOD) to strengthen plans and capabilities for coordinated operations.

Close coordination will also be necessary with Canada. The secretary of energy has no authority to issue emergency orders to power companies in other countries. However, the electric grids of the United States and Canada are deeply interconnected. This integration entails both risks and opportunities in grid security emergencies. Adversary-induced blackouts in one nation may cascade across the border, and extraordinary measures taken to restore US grid reliability could affect Canadian systems. Yet, the connectivity between US and Canadian electric systems can also provide unique opportunities to strengthen the security and emergency preparedness of both nations.

A key foundation for binational cooperation in grid security emergencies is already in place. NERC's reliability standards apply to both US and Canadian utilities, providing shared planning and emergency coordination mechanisms on both sides of the border. US and Canadian power companies and government officials should explore how they might supplement these existing mechanisms for grid security emergencies. The most immediate opportunity to do so will lie in government-to-government consultations. The FPA requires that, to the extent practicable, the secretary of energy shall consult with Canadian authorities before issuing emergency orders.[274] However, the FPA provides no details on the mechanisms by which consultations will be conducted or on whether and how Canadian officials should be informed when the secretary issues emergency orders to US utilities. The analysis that follows examines opportunities to facilitate binational consultation and operational coordination in grid security emergencies.

The FPA also requires that the secretary consult with the Mexican government before issuing emergency orders. While the US and Mexican grids are much less integrated than those of the US and Canada, discussions on grid security emergency preparedness with Mexican officials could also be valuable. Coordination beyond North America may be useful as well. If a severe regional crisis escalates into attacks on the US power grid, US security partners in those regions may face strikes against their own electric systems. Sharing information on whether an attack is imminent and taking coordinated grid protection measures (including those for conservative operations) will help the United States and its allies meet such challenges.

Deepening Integration between US and Canadian Grids: Risks and Potential Benefits for Grid Security Emergency Resilience

DOE notes that "the United States and Canada serve as a global model of highly functional, cross-border electricity coordination."[275] US and Canadian grids are connected by over three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north–south BPS infrastructure and synchronized

[273] 16 U.S.C. § 824o–1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

[274] 16 U.S.C. § 824o–1, (b)(3).

[275] DOE, *Quadrennial Energy Review: Second Installment*, 6-5.

cross-border operations.[276] This integration also provides significant economic and energy security benefits for both countries.[277]

Connectivity between US and Canadian grids will grow still closer in the decades to come.[278] New York and Massachusetts are pursuing significant increases in Canadian hydropower to help achieve their clean energy goals. Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2020.[279] The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2021, with still other projects in various phases of development in New England, the Midwest, and the Pacific Northwest.[280]

These and other projects offer significant economic benefits to both nations. However, the connectivity of US and Canadian power grids also creates risks of cross-border failures. The 2003 Northeast blackout that started in Ohio created power outages for millions of customers in Ontario.[281] Interconnections between US and Canadian power systems have increased since that event. US and Canadian officials warn that given this connectivity, "isolated or complex events with cascading effects that take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety."[282]

[276] DOE, *Quadrennial Energy Review: Second Installment*, 6-6.

[277] Stanley, *Mapping the U.S.-Canada Energy Relationship*, 9.

[278] Parfomak et al., *Cross-Border Energy Trade*, 34.

[279] "Work Continues on ITC Lake Erie Project," *Transmission Hub*.

[280] Vine, *Interconnected: Canadian and U.S. Electricity*, 9.

[281] NERC Steering Group, *Technical Analysis of Blackout*, 1.

[282] Governments of US and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, 10.

Mandatory reliability standards reduce the risks of outages across North America. In the aftermath of the 2003 blackout, NERC began issuing standards applicable to entities on both sides of the border. NERC reliability standards are mandatory and enforceable in the provinces of Ontario, New Brunswick, Alberta, British Columbia, Manitoba, and Nova Scotia. Twelve such reliability standards also went into effect in Quebec in April 2015; the province is now considering adopting additional standards.[283] These shared US–Canada standards help power companies in both countries maintain the reliability of their systems and will help them prevent instabilities from spreading during grid security emergencies.

NERC's role as the electric reliability organization for North America provides an additional bulwark for binational grid resilience. As Figure 7 illustrates, three NERC regional entities include power companies on both sides of the border: the Northeast Power Coordinating Council (NPCC), the Midwest Reliability Organization (MRO), and the Western Electricity Coordinating Council (WECC). These entities help monitor and enforce compliance with reliability standards and reinforce NERC's integrated approach to reducing the risks of cascading failures and other instabilities.[284] The E-ISAC also provides additional support for utility preparedness in both nations.

However, Russia and other potential adversaries' increasingly sophisticated cyber capabilities pose challenges for protecting power flows between Canada and the United States, just as they do for electric service within each country individually.

Connectivity between US and Canadian power systems offers other benefits for protecting reliability against cyber and physical attacks. For example, as

[283] "North America," NERC. See also "Compliance - Québec," Northeast Power Coordinating Council; and "Electric Power Transmission Reliability Standards," Régie de l'énergie Québec.

[284] "Key Players," NERC.

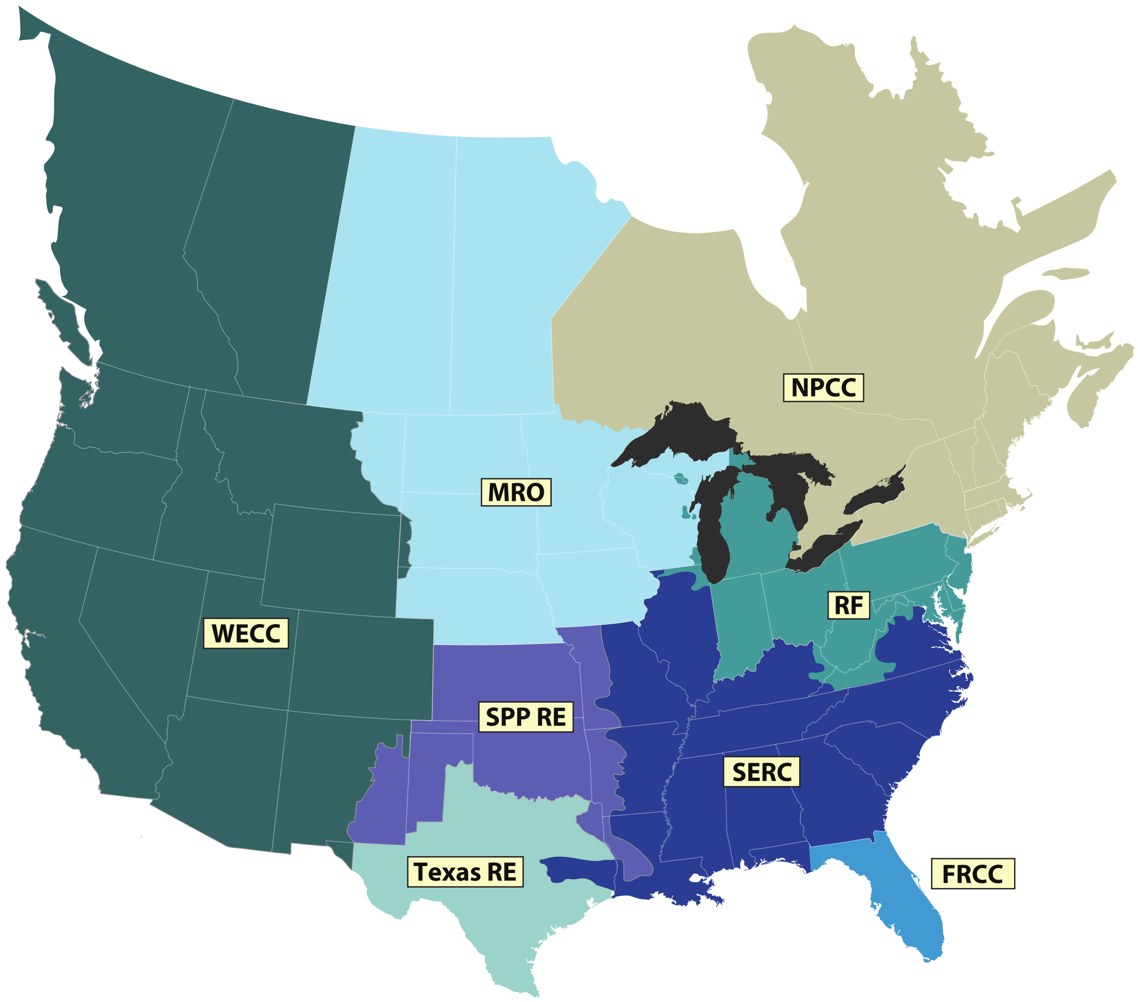

Figure 7. NERC Regional Entities across North America

new transmission lines increase this connectivity, electricity exported by Canada could become increasingly valuable when managing power imbalances in the United States and could make up for sudden shortfalls in the availability of US-generated power. However, we must assume that adversaries know this as well. To maximize the disruption to the US grid and the critical facilities that depend on it, attackers may strike the cross-border transmission lines that would otherwise help US grid owners and operators prevent cascading failures, uncontrolled separations, and other major reliability issues.

Adversaries may also attack grid assets that supply power to critical Canadian defense installations. The United States and Canada have a unique binational defense system to protect their territories. The North American Aerospace Defense Command plays a vital role for both nations for aerospace warning, aerospace control, and maritime warning for North America.[285] The Canada-US Civil Assistance Plan also helps enable military members from one nation assist the other's armed forces in support of civilian authorities during emergencies.[286] Potential adversaries such as Russia may seek to degrade these binational military capabilities and operations by attacking defense critical electric infrastructure on

[285] "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

[286] "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

both sides of the border. US and Canadian officials and power companies should plan accordingly for mutual support in grid security emergencies.

Specific Options for US–Canada Coordination

In addition to requiring US–Canada consultations before the secretary issues emergency orders, the FPA also states that FERC and the secretary "shall, in consultation with Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk-power system outside the United States."[287] Those initiatives provide a valuable starting point to build shared North American preparedness for grid security emergencies. However, much deeper collaboration is both possible and necessary, especially with Canada. Options for further analysis are described below.

Consultative mechanisms, collaborative planning, and coordinated emergency operations. The FPA does not specify how US officials would consult with their Canadian counterparts if the president declares a grid security emergency. Nor does it discuss whether the president would do so prior to making such a declaration. Exchanges between the US president and the prime minister of Canada would constitute the highest level of binational coordination. More detailed discussions about options for responding to incidents could also occur between the secretary of energy and the Canadian minister of national resources. That minister has the federal lead for electricity issues in Canada but lacks emergency authorities equivalent to those that the FPA grants to the secretary of energy.[288]

However, government coordination mechanisms will also need to include a broader array of participants. Global Affairs Canada and the US State Department might well be involved in any coordination of binational grid emergency actions, just as they are in other emergency assistance mechanisms.[289] Coordination with state and provincial governments could also be helpful. The 1982 amendments to Canada's Constitution Act (1867) explicitly recognized provinces' and territories' constitutional rights to manage electrical energy.[290] In particular, authority over electricity generation and transmission in Canada rests primarily with provincial governments.[291] It will be essential to account for these features of Canadian governance in building US–Canada consultative mechanisms.

The NERC alert system and other emergency coordination systems provide a solid basis for collaboration between US and Canadian utilities in grid security emergencies. However, the FPA does not address the question of how (and how much) information DOE officials should share with Canada on the issuance of emergency orders to US utilities. Given the deep integration of the US and Canadian grids, maximum sharing could help coordinate both countries' emergency operations before, during, and after attacks. To facilitate such information sharing, DOE, Natural Resources Canada, and other relevant stakeholders can leverage existing US–Canadian mechanisms to protect sensitive information, supplemented as needed to support grid security emergency coordination.

The *Joint US-Canada Electric Grid Security and Resilience Strategy* (December 2016) provides a policy framework for building these coordination and information sharing mechanisms. The US and Canadian governments developed the strategy "to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats."[292] The strategy calls for collaboration to protect system assets and

[287] 16 U.S.C. § 824o–1, (d)(5).

[288] "Roles and Responsibilities," Natural Resources Canada.

[289] "Compendium," Public Safety Canada.

[290] "Roles and Responsibilities," Natural Resources Canada.

[291] "North America," NERC.

[292] Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 1.

critical functions in both nations so that the North American grid can "withstand and recover rapidly from disruptions."[293] The strategy also emphasizes the need for collaboration to manage contingencies and enhance response and recovery efforts.[294] All of these features make the strategy a promising basis for creating the detailed collaborative mechanisms that grid security emergencies will require.

Protecting defense critical electric infrastructure. While the FPA facilitates the development of emergency orders to protect the flow of power to critical US defense installations, US–Canada coordination in grid security emergencies could also help strengthen power resilience for bases on both sides of the border. The Pacific Northwest exemplifies the potential benefits of such collaboration. Washington State hosts a number of vital installations, including Joint Base Kitsap on Puget Sound, which serves as the homeport for aircraft carriers, attack submarines, and other assets that would be needed for operations in the South China Sea and for other regional contingencies. Canadian Forces Base Esquimalt and other key Canadian installations are located less than one hundred miles away on Vancouver Island. Esquimalt is the second-largest military base in Canada and is home to Maritime Forces Pacific and Joint Task Force Pacific headquarters.[295] Coordinating US–Canada emergency plans to protect the flow of power to these installations could benefit the security of both nations.

The US–Canada Permanent Joint Board on Defense provides an ideal venue to explore such coordination options. Established in 1940 to discuss and advise on issues related to continental defense and security, the board has focused increasing attention on binational opportunities to strengthen critical infrastructure resilience. In 2011, the CEO of NERC led a Permanent Joint Board on Defense discussion of how North American BPS emergency plans and coordination mechanisms could benefit US and Canadian national security. Natural Resources Canada and DOE have also participated in subsequent Permanent Joint Board on Defense meetings, along with the defense departments of both nations and critical infrastructure stakeholders. US and Canadian officials should consider using the board to facilitate industry–government discussions on opportunities to coordinate in grid security emergencies.

Coordination with Mexico and Beyond: Multinational Resilience against Grid Security Emergencies

The US grid has much less connectivity with Mexican electric systems than with the Canadian grid. Southern California and a portion of Mexico's Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities.[296] In 2017, Mexican and US officials agreed to nonbinding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.[297]

The election of Mexican president Andrés Manuel López Obrador in July 2018 may lead to significant changes in that country's energy policies.[298] Structural challenges will also slow efforts to increase US–Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.[299] Nevertheless, it could be useful to expand discussions with industry and the incoming government on protecting grid reliability against cyber and physical threats.

[293] Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 12.

[294] Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 11.

[295] "Maritime Forces Pacific," Royal Canadian Navy.

[296] DOE, *Quadrennial Energy Review: Second Installment*, 6-4.

[297] "Increasing Electricity Cooperation in North America," DOE.

[298] Kissane and Medina, "Energy Aftershocks."

[299] DOE, *Quadrennial Energy Review: Second Installment*, 6-13.

Building grid security emergency coordination mechanisms beyond North America would also be helpful. As noted earlier, attacks on the US grid are most likely to occur in the context of an intense, escalating regional crisis in the Baltics, Northeast Asia, or some other area where US allies and critical security interests are at risk. In particular, adversaries may seek to inflict blackouts that could disrupt the deployment of US forces to the crisis zone. But we should also expect that US allies in the region will suffer attacks on their own grids, aimed at disrupting their ability to conduct combined operations with the United States and deliver electricity to US bases on their territories.

NATO's 2018 Locked Shields exercise focused on building alliance-wide preparedness for cyber and physical attacks against energy and communications systems.[300] In future exercises, allies might explore how to jointly determine whether grid attacks are potentially imminent and coordinate on the implementation of conservative operations across NATO member countries. The United States might explore equivalent opportunities for collaboration with Japan, South Korea, Australia, New Zealand, and other security partners. Existing treaty commitments, including those under Article V of NATO's founding treaty, will provide a starting point to meet our shared grid resilience challenges.[301]

Playing Defense in Cyberwarfare: Doctrine, Integrated Planning, and Benefits for Deterrence

Utility leaders are urging the federal government to do more to assist them in deterring and defeating attacks on the grid. Their calls come at a perfect time. Administration officials have opened the door to new forms of operational collaboration between industry and government, including "collective defense" during cyber attacks.[302] This report examines an especially significant option to expand their collaboration: coordinating the implementation of emergency orders with DOD operations to halt attacks at their source.

Deeper operational partnerships can also help meet underlying challenges for cyber deterrence. A number of cybersecurity analysts argue that deterrence by denial is impractical in cyberspace because offensive cyber capabilities are so much stronger than cyber defenses, and because cyber warfare will be very different from conventional conflicts. Analysts also warn that the United States lives in a cyber "glass house": given the vulnerability of the power grid and other infrastructure systems, the president cannot credibly threaten to use cyber weapons to defend US allies and interests. Improving preparedness for grid security emergencies can help address these concerns and support ongoing reassessments of US strategies for deterrence.

Unity of Effort in Defensive Operations at Home and Abroad

Tom Fanning, CEO of Southern Company (one of the largest power companies in the United States), notes that he and other infrastructure owners and operators face a major constraint on their ability to defend their systems: "I can't fight back."[303] In theory, blunting attacks at their source could greatly ease the scale and severity of the threats that utilities will need to counter. In practice, integrating grid security emergency operations with measures to suppress enemy attacks would entail major policy and technical obstacles.

Power companies should not be responsible for striking enemies' offensive cyber infrastructure during grid security emergencies. The US government is the sole actor with the prerogative to engage in techniques such as "hacking back" that

300 Cowan, "Locked Shields 2018."

301 "The North Atlantic Treaty," NATO.

302 Nielsen, *National Cybersecurity Summit Keynote Speech*.

303 Smith, "U.S. Officials Push New Penalties."

involve operations to disrupt or destroy an attacker's system.[304] Moreover, even if power companies gained legal authority to fight back against adversaries, their technical capacity to do so would be dwarfed by the capabilities possessed by US Cyber Command and other US government organizations.

Efforts to integrate defensive operations at home and abroad should rest on the comparative advantages of industry and government. BPS entities and other components of the electricity subsector are best positioned to defend their systems from within, assisted by DOE and other government partners. Operations abroad to halt attacks on the grid should remain the exclusive purview of government agencies, supported by industry assistance to gather malware samples and facilitate attack attribution. Based on this division of labor, government and industry leaders could explore whether and how to strengthen unity of effort for the full scope of defensive operations within the United Sates and beyond.

Secretary of homeland security Kirstjen Nielsen has called for the adoption of a "collective defense" posture that might include such expanded partnerships. Under the collective defense model, industry and government would collaborate to act on threat indicators and "respond more quickly and effectively to incidents."[305] The most familiar realm of operational collaboration lies in government support to help utilities detect, characterize, and eradicate malware on their systems. DHS is strengthening the National Cybersecurity and Communications Integration Center's ability to provide such assistance.[306] State National Guard organizations can also support post-cyber attack power restoration within the larger context of the industry's Cyber Mutual Assistance system.[307] However, in a cyber strike against the United States, DOD will require many of these same guard personnel to protect the department's networks, conduct cyber operations against the attacker, and carry out other federal missions.[308] Power companies and government agencies will need to continue clarifying whether and how specific National Guard assets can help meet utility requests for assistance; existing doctrine and procedures for providing defense support to civil authorities offer a solid basis to advance those discussions.

In contrast, coordinating industry grid protection measures with government operations to suppress attacks would extend collective defense into uncharted territory. The command vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, offers a starting point to examine how engaging against malicious cyber actors might help protect utilities. The document states that the United States must "increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." To do so, DOD "is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems."[309]

Forward defense operations could respond to and help counter adversary efforts to implant malware on utility networks. Should such operations also help power companies protect their systems if the president declares that an attack is imminent? As senator Mike Rounds frames the question: "If someone is going to shoot an arrow at you, do you shoot the archer before he shoots the arrow?"[310]

US Cyber Command's vision statement does not directly address this possibility. However, each phase of grid security emergencies will likely offer

[304] GWU, *Into the Gray Zone*, 25.

[305] Nielsen, *National Cybersecurity Summit Keynote Speech*.

[306] Marks, "DHS Stands Up New Cyber Risk Center."

[307] Crowe, "National Guard Preparing"; and Puryear, "91st Cyber Brigade Activated."

[308] DOD, *Cyber Strategy*, 4.

[309] US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4–5.

[310] Bordelon, "Rounds Is Ready."

a different mix of risks and rewards for combining domestic and forward defense operations. For example, if the president determines that an attack on the grid is imminent, the secretary might issue orders for conservative operations to bolster grid defenses at the same moment that forward defense operations disrupted enemy cyber infrastructure poised to launch the strike. But assessments that an attack is imminent may turn out to be wrong. No-regrets orders for conservative operations are valuable precisely because using them will entail few consequences if warning indicators turn out to be false. Preattack forward defense operations could start a cyberwar that might not otherwise have occurred.

The United Sates can avoid such risks by waiting until attacks on the grid are under way before striking the enemy's offensive infrastructure. However, developing the technical capabilities to identify and disrupt the cyber infrastructure being used in an attack could prove challenging. Moreover, it is not clear whether integrating plans for home and away operations would offer significant benefits, as opposed to relying on utilities and government agencies to conduct those two types of operations independently.

US Cyber Command has opened the door to building new types of partnerships with the electricity subsector. The command has called for measures to "deepen and operationalize" collaboration between the private sector, the armed services, and other command partners.[311] As those efforts go forward with the electricity subsector and DOE, exploring options for collective defense (and clarifying the dangers they might present) should be a prime focus for analysis.

Maximizing Industry Contributions to Cyber Deterrence by Denial

The *National Security Strategy* emphasizes that rather than rely on threats of cost imposition alone to deter enemy attacks, the United States will also strengthen deterrence by denial. This report has examined how grid security emergency orders and implementation plans can raise adversaries' doubts as to whether they can achieve their objectives. But strengthening this form of deterrence will also entail underlying challenges.

Many cybersecurity analysts believe that offensive cyber capabilities are vastly stronger than defenses against them, and that this preeminence creates destabilizing incentives for adversaries to strike first when conflicts loom.[312] Unless measures to strengthen grid resilience can help weaken the dominance of offense over defense in the cyber realm, deterrence by denial will remain difficult to accomplish against highly capable adversaries.

However, today's offensive dominance stems in part from historical factors that are rapidly changing. The interconnected grid evolved decades ago when no cyber threat existed to drive protective measures. Moreover, as utilities began incorporating computer-assisted controls, sensors, and operating technology systems, few of these companies accounted for the risk that cyber threats to their systems would escalate so rapidly. As noted in this report, utilities are advancing a wide array of technical initiatives and fallback operational plans to counter and (ideally) stay ahead of adversaries' capabilities. In addition, regulatory bodies across the nation are increasingly willing to enable companies to recover costs for cyber resilience.

The current preeminence of offense over defense also reflects organizational factors. Rebecca Slayton has found that historically, "the success of offense is largely the result of a poorly managed defense."[313] The skills of the individuals employing cyber weapons and defensive tools, and the effectiveness with which

311 US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 8.

312 For a review of this "offense-dominant" literature, and the smaller set of works opposing it, see Slayton, "What Is the Cyber Offense-Defense Balance?," 72.

313 Slayton, "What Is the Cyber Offense-Defense Balance?," 87.

these practitioners are managed and organized, have an enormous impact on the outcome of cyber engagements. Slayton notes that the importance of organization for cyber defense is implicit in discussions of the need for better public–private partnerships and information sharing. What has been missing, however, are efforts to make such partnerships *operational* and create unity of effort in government–industry defense actions when adversaries strike. That is precisely the gap that DOE and its industry partners can fill by developing grid security emergency orders and advancing all of the other collaborative initiatives necessary to make those orders effective.

Improved partnerships and technical capabilities to protect the grid cannot by themselves make defense preeminent. To further rebalance offense and defense in cyberspace, resilience initiatives will be necessary across all critical infrastructure sectors, as well as a host of other measures to facilitate the command, control, and coordination of public–private defensive operations. But building preparedness for grid security emergencies will be vital for that broader effort. Moreover, establishing defensive primacy is not necessary to facilitate deterrence by denial. As defined by the *National Security Strategy*, deterrence by denial functions by creating doubt in our adversaries that they can achieve their objectives.[314] DOE and its partners should develop grid security emergency orders that (perhaps in conjunction with forward defense operations) can make adversaries less likely to attack, even if defensive dominance remains out of reach.

Strengthening grid resilience can also support the broader reassessment of the US deterrence posture that is now under way. Robert Strayer, the State Department's deputy assistant secretary for cyber and international communications and information policy, notes that the increasing severity of threats to US infrastructure is forcing "an evolution in the US government's thinking about how to deter malicious cyber actors."[315] In conventional warfare, deterrence by denial functions by making it physically difficult for adversaries to achieve their objectives and by raising enemy forces' costs of taking their targets.[316] Cyberwarfare will not entail the same sorts of attrition of enemy forces that occurs in battles with tanks, fighter aircraft, and other conventional weapons. The Trump and Obama administrations have redefined deterrence by denial to better fit the characteristics of cyberspace. The unique features of cyber conflict will require continued rethinking of how the United States can strengthen deterrence in the years to come. As utilities and government agencies build resilience for grid security emergencies, new opportunities will emerge to influence adversaries' perceived costs and benefits of attack. The United States should continue to refine its deterrence posture to capitalize on these improvements.

Escaping the "Glass House" Syndrome

The president may need the ability to use cyber weapons against foreign targets to help resolve crises on terms favorable to the United States. The *DOD Cyber Strategy* (April 2015) states that:

> There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an

314 White House, *National Security Strategy*, 13.

315 Smith, "U.S. Officials Push New Penalties."

316 For definitions of classic deterrence by denial derived from conventional warfare, see Gerson, "Conventional Deterrence"; and Mitchell, "The Case for Deterrence by Denial." For an analysis of how that definition differs from that used by the Trump administration, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy."

> ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.[317]

However, any such operations against an adversary's cyber infrastructure would risk retaliatory strikes against the United States—including, potentially, attacks on the grid. Senator Thom Tillis (R-NC), a member of the Senate Armed Service Committee, emphasizes that the United States is living in "a big glass house."[318] If US infrastructure owners and operators cannot defend their systems against attack, the president may be reluctant to use cyber weapons abroad, even if doing so might otherwise offer enormous benefits for conflict termination. In short: US leaders may be self-deterred from taking actions that they may need to employ. Developing emergency orders and implementation plans to protect grid reliability could reduce these glass house constraints and widen the range of options available for the president to protect US interests.

Improving grid defenses could also help strengthen the credibility of US commitments to defend key allies. Former US defense and intelligence officials have proposed that the United States and other high-cyber-capability NATO allies provide extended deterrence against cyber attacks for less capable alliance members.[319] But glass house concerns would call into question the credibility such commitments. Measures to strengthen grid resilience could help convince adversaries that the United States is willing to help allies respond to cyber attacks on their infrastructure.

Yet, nothing requires the United States to respond to such attacks with cyber weapons alone. On the contrary: the *National Security Strategy* and other policy documents leave open the possibility that if cyber attacks at home or abroad are sufficiently severe, the United States will respond with conventional or even nuclear weapons. James Lewis notes that "opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return," and will surely weigh that risk given "the immense capacity of the United States to inflict punishment" on attackers.[320] Emergency orders to protect the flow of power to defense installations can and should reinforce the certainty of that punishment.

But any first use of cyber weapons by the United States would entail escalatory dangers as well. If the United States were to initiate the use of destructive cyber weapons to defend US allies and interests, potential adversaries such as Russia could respond with conventional or nuclear forces. Moreover, conflicts that begin with the large-scale use of cyber weapons could also spiral out of control in ways that neither side desires or anticipates.[321] These escalatory risks must be in the forefront of calculations on whether and how to engage in cyber warfare. Indeed, as government agencies partner with power companies to build resilience for grid security emergencies, deterring such conflicts and reducing the likelihood of cyberwarfare should always be our prime objective.

317 DOD, *Cyber Strategy*, 5.

318 Schwartz, "Sen. Tillis: We Are Living in a Glass House." For additional analysis of the glass house syndrome and its effects on constraining US options, see Miller, "Cyber Deterrence"; and Rosenbach, "Living in a Glass House."

319 Kramer, Butler, and Lotrionte, *Cyber, Extended Deterrence, and NATO*, 1.

320 Lewis, *Rethinking Cybersecurity*, 9, 29. The author also argues that even if attacks on the grid occur, they would be unlikely to achieve the strategic effects that adversaries will seek, further reducing the likelihood of such attacks (see pp. 21 and 24–26).

321 Danzig, *Surviving on a Diet of Poisoned Fruit*, 25; Lin, "Escalation Dynamics," 52; and Miller and Fontaine, *A New Era*, 18–20.

Bibliography

6 U.S.C. § 124l. https://www.law.cornell.edu/uscode/text/6/124l.

15 U.S.C. § 3361. https://www.law.cornell.edu/uscode/text/15/3361.

15 U.S.C. § 3363. https://www.law.cornell.edu/uscode/text/15/3363.

15 U.S.C. § 3364. https://www.law.cornell.edu/uscode/text/15/3364.

16 U.S.C. § 824a. https://www.law.cornell.edu/uscode/text/16/824a.

16 U.S.C. § 824o. https://www.law.cornell.edu/uscode/text/16/824o.

16 U.S.C. § 824o–1. https://www.law.cornell.edu/uscode/text/16/824o–1.

18 CFR 388.113. https://www.law.cornell.edu/cfr/text/18/388.113.

47 U.S.C. § 606. https://www.law.cornell.edu/uscode/text/47/606.

50 U.S.C. Appendix §2071(c). https://law.justia.com/codes/us/2001/title50/app/defensepr/sec2071/.

“About Alerts.” NERC (North American Electric Reliability Corporation). n.d. http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx.

“About NERC.” NERC (North American Electric Reliability Corporation). n.d. http://www.nerc.com/AboutNERC/Pages/default.aspx.

“About NSTAC.” DOS (US Department of State). Last published June 20, 2016. https://www.dhs.gov/about-nstac.

“About 60% of the U.S. Electric Power Supply Is Managed by RTOs.” US Energy Information Administration. April 4, 2011. https://www.eia.gov/todayinenergy/detail.php?id=790.

“Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E).” ICS-CERT. Originally released December 10, 2014, last revised December 9, 2016. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

“Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure.” ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). February 25, 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

“Alert (TA17-163A): CrashOverride Malware.” US-CERT (US Computer Emergency Readiness Team). June 12, 2017. https://www.us-cert.gov/ncas/alerts/TA17-163A.

“Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). October 20, 2017. https://www.us-cert.gov/ncas/alerts/TA17-293A.

“Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

ASD(EI&E) (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment). *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*. Washington, DC: DOD, July 2017. https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf.

Assante, Michael, and Robert M. Lee. *The Industrial Control System Cyber Kill Chain*. Bethesda, MD: SANS Institute, October 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

"Automated Indicator Sharing (AIS)." US-CERT (US Computer Emergency Readiness Team). n.d. https://www.us-cert.gov/ais.

Banham, Russ. "DDoS Attacks Evolve to Conscript Devices onto the IoT." *Forbes*, February 4, 2018. https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#-4b5a43a86aaa.

Barnes, Julian E. "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks." *New York Times*, July 13, 2018. https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html.

Blue Ribbon Study Panel on Biodefense (Hudson Institute). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts—A Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Hudson Institute, October 2015. http://www.biodefensestudy.org/a-national-blueprint-for-biodefense.

Bordelon, Brendan. "Rounds Is Ready to Lead New Senate Cybersecurity Subcommittee." *Morning Consult*, February 1, 2017. https://morningconsult.com/2017/02/01/rounds-ready-lead-new-senate-cybersecurity-subcommittee/.

Brown, Jared T., and Daniel H. Else. *The Defense Production Act of 1950: History, Authorities, and Reauthorization*. Washington, DC: Congressional Research Service, July 28, 2014. https://fas.org/sgp/crs/natsec/R43118.pdf.

"The Canada-U.S. Defence Relationship." Department of National Defence and the Canadian Armed Forces. December 4, 2014, last modified February 10, 2015. http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s.

Cherepanov, Anton, and Robert Lipovsky. "Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet." *WeLiveSecurity* (ESET Blog), June 12, 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

"Compendium of U.S.-Canada Emergency Management Assistance Mechanisms." Public Safety Canada. October 2016, last modified March 28, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmpndm-ntdstts-cnd-2016/index-en.aspx.

"Compliance - Québec." Northeast Power Coordinating Council. n.d. https://www.npcc.org/Compliance/Quebec/Forms/Public%20List.aspx.

Cowan, Gerrard. "Locked Shields 2018 Practises for Large-Scale Cyber Incident." *Jane's 360*, April 29, 2018. http://www.janes.com/article/79652/locked-shields-2018-practises-for-large-scale-cyber-incident.

Crowe, Greg. "National Guard Preparing to Defend Cyberspace for States." *Federal News Radio*, April 16, 2018. https://federalnewsradio.com/cyber-exposure/2018/04/national-guard-preparing-to-defend-cyberspace-for-states/.

"Cybersecurity." American Gas Association. n.d. https://www.aga.org/safety/security/cybersecurity/.

"The Cyber Threat Framework." ODNI (Office of the Director of National Intelligence). n.d. https://www.dni.gov/index.php/cyber-threat-framework.

Danzig, Richard. *Catastrophic Bioterrorism—What Is to Be Done?* Washington, DC: Center for Technology and National Security Policy, August 2003. http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf.

———. *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, July 2014. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf.

Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: DOD, February 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf.

DHS (US Department of Homeland Security). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: DHS, December 17, 2003. https://www.dhs.gov/homeland-security-presidential-directive-7.

———. *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

———. *National Response Framework*. 3rd ed. Washington, DC: DHS, June 2016. https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf.

———. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

———. *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage*. Washington, DC: DHS, June 2017. https://www.fema.gov/media-library/assets/documents/154058.

———. *Strategy for Protecting and Preparing the Homeland against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. Washington, DC: DHS, forthcoming.

———. *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: DHS, May, 15, 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

DiSavino, Scott, and David Sheppard. "ConEd Cuts Power to Part of Lower Manhattan Due to Sandy." *Reuters*, October 29, 2012. https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030.

DOD (US Department of Defense). *Department of Defense Manual 3020.45*. Washington, DC: DOD, last updated May 23, 2017. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf.

———. *DoD Cybersecurity Discipline Implementation Plan*. Washington, DC: DOD, amended February 2016. http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf.

———. *DOD Cyber Strategy.* Washington, DC: DOD, April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

———. *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DOD, November 29, 2016. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf.

———. *Mission Assurance Strategy*. Washington, DC: DOD, April 2012. http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

DOE (US Department of Energy). “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40).” *Federal Register* 83, no. 7 (2018): 1176. https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance.

———. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, DC: DOE, February 2014. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

———. *Electromagnetic Pulse Resilience Action Plan*. Washington, DC: DOE, January 2017. https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf.

———. “Energy Priorities and Allocations System Regulations (RIN 1901–AB28).” *Federal Register* 76, no. 111 (2011): 33615. https://www.gpo.gov/fdsys/pkg/FR-2011-06-09/pdf/2011-14282.pdf.

———. *Multiyear Plan for Energy Sector Cybersecurity*. Washington, DC: DOE, March 2018. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

———. *Quadrennial Energy Review—Transforming the Nation’s Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf.

———. *Staff Report to the Secretary on Electricity Markets and Reliability*. Washington, DC: DOE, August 2017. https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf.

———. *Strategic Transformer Reserve: Report to Congress*. Washington, DC: DOE, March 2017. https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

“DOE’s Use of Federal Power Act Emergency Authority.” DOE (US Department of Energy). n.d. https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use.

DOS (US Department of State). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: DOS, May 31, 2018. https://www.state.gov/documents/organization/282253.pdf.

Dougherty, Jon. "Biggest U.S. Power Grid Operator Suffers Thousands of Attempted Cyber Attacks per Month." *Forward Observer*, August 28, 2017. https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/.

Douris, Constance. "DARPA Research Leads Grid Security Solutions." *The Buzz* (blog), *National Interest*, January 12, 2017. http://nationalinterest.org/blog/the-buzz/darpa-research-leads-grid-security-solutions-19044.

Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

EEI (Edison Electric Institute). "Comments of the Edison Electric Institute." In *Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*. February 6, 2017.

———. *Understanding the Electric Power Industry's Response and Restoration Process*. Washington, DC: EEI, October 2016. http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf.

EIS Council (Electric Infrastructure Security Council). *E-PRO Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf.

———. *E-PRO Handbook III: Black Sky Cross-Sector Coordination and Communication*. Washington, DC: EIS Council, June 2018. https://www.eiscouncil.org/EPRO_Books.aspx.

E-ISAC (Electricity Information Sharing and Analysis Center) and SANS-ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: NERC, March 2016. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

"Electricity Information Sharing and Analysis Center." NERC (North American Electric Reliability Corporation). n.d. http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

"Electric Power Transmission Reliability Standards Compliance Monitoring and Enforcement." Régie de l'énergie Québec. n.d. http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html.

"Emergency Communications." DHS (US Department of Homeland Security). Last published June 26, 2018. https://www.dhs.gov/topic/emergency-communications.

Energy Policy Act of 2005. Public Law 109-58. *U.S. Statutes at Large* 119 (2005): 942–943. https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119.pdf.

"Energy Sector Cybersecurity Preparedness." DOE (US Department of Energy). n.d. https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0.

EPRI (Electric Power Research Institute). *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*. Report 3002000796. Palo Alto, CA: EPRI, December 2013. https://publicdownload.epri.com/PublicDownload.svc/product=000000003002000796/type=Product.

———. *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs*. Report 3002008999. Palo Alto, CA: EPRI, September 2016. https://www.epri.com/#/pages/product/000000003002008999/?lang=en.

ESCC (Electricity Subsector Coordinating Council). *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: DHS, August 5, 2013. https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf.

"ESCC: Electricity Subsector Coordinating Council." ESCC (Electricity Subsector Coordinating Council). January 2018. http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8.

"The ESCC's Cyber Mutual Assistance Program." ESCC (Electricity Subsector Coordinating Council). January 2018. http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1.

FEMA (US Federal Emergency Management Agency). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: FEMA, July 12, 2018. https://www.fema.gov/media-library/assets/documents/167249.

FERC (Federal Energy Regulatory Commission). *Cyber Security Incident Reporting Reliability Standards*. 161 FERC ¶ 61,291. December 21, 2017. https://www.ferc.gov/whats-new/comm-meet/2017/122117/E-1.pdf.

———. *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies, Statement of Policy*. 96 FERC ¶ 61,299. September 14, 2011.

———. *Grid Resilience in Regional Transmission Organizations and Independent System Operators*. 162 FERC ¶ 61,256. 2018. https://www.ferc.gov/CalendarFiles/20180320102618-AD18-7-000.pdf.

———. *Order Authorizing Acquisition and Disposition of Jurisdictional Facilities*. 163 FERC ¶ 61,005. April 3, 2018. https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf.

———. *Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool Regional Entity.* 163 FERC ¶ 61,094. May 4, 2018. https://www.ferc.gov/CalendarFiles/20180504141902-RR18-3-000.pdf.

———. *Policy Statement on Matters Related to Bulk Power System Reliability*. 107 FERC ¶ 61,052. April 19, 2004. https://www.ferc.gov/whats-new/comm-meet/041404/E-6.pdf.

———. *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833. 157 FERC ¶ 61,123. November 17, 2016. https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-4.pdf.

———. *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833-A. 163 FERC ¶ 61,125. May 17, 2018. https://www.ferc.gov/whats-new/comm-meet/2018/051718/E-2.pdf.

———. *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*. 156 FERC ¶ 61,215. September 22, 2016. https://www.ferc.gov/whats-new/comm-meet/2016/092216/E-4.pdf.

———. *Revision to Electric Reliability Organization Definition of Bulk Electric System*. Order No. 743. 133 FERC ¶ 61,150. November 18, 2010. https://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf.

———. *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. Order No. 773-A. 143 FERC ¶ 61,053. April 18, 2013. https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf.

FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. Washington, DC: FERC, January 2016. https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf.

———. *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*. Washington, DC: FERC, June 2017. https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf.

———. *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Recommended Study: Blackstart Resources Availability (BRAv)*. Washington, DC: FERC, May 2018. https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (2017): 381–393. https://www.sciencedirect.com/science/article/pii/S0030438717300431.

Fixing America's Surface Transportation Act, Public Law 114-94. *U.S. Statutes at Large* 129 (2015): 1773–1774. https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf.

Frankel, Alison. "Can Customers Sue Power Companies for Outages? Yes, but It's Hard to Win." *Reuters* (blog), November 9, 2012. http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/.

Galloway, T .J., Sr. "Advancing Reliability and Resilience of the Grid." Comments presented at the FERC Reliability Technical Conference, Washington, DC, July 31, 2018. https://www.ferc.gov/CalendarFiles/20180731084251-Galloway,%20North%20American%20Transmission%20Forum.pdf.

Gerson, Michael S. "Conventional Deterrence in the Second Nuclear Age." *Parameters* 39 (Autumn 2009): 32–48. https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf.

Governments of the US and Canada. *Joint United States-Canada Electric Grid Security and Resilience Strategy*. Washington, DC: The White House, December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf.

GWU (George Washington University) Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: GWU, October 2016. https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Healy, Jason. *The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities*. SSRN, June 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206.

Homeland Security Advisory Council. *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DOS, June 2016. https://www.hsdl.org/?view&did=794271.

ICF. *Assessment of Large Power Transformer Risk Mitigation Strategies*. Fairfax, VA: ICF, October 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf.

———. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Fairfax, VA: ICF, June 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

"Increasing Electricity Cooperation in North America." DOE (US Department of Energy). January 11, 2017. https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america.

INL (Idaho National Laboratory). *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*. Idaho Falls, IN: INL, January 2016. https://inldigitallibrary.inl.gov/sites/STI/STI/INL-EXT-15-35582.pdf.

ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf.

———. "Response of ISO New England Inc." *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000). March 9, 2018. https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7_iso_response_to_grid_resilience.pdf.

Jenkins, Brian Michael. "Countering al-Qaeda: The Next Phase in the War." *The RAND Blog*, September 8, 2002. https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html.

Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, July 12, 2017. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

Joint Commenters. "Comments of American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group." In *Response to RIN 1901–AB40*. February 23, 2017. http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf.

Kaften, Cheryl. "DoD Tests Energy Continuity with 'Islanded' Microgrid." *Energy Manager Today*, April 5, 2017. https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/.

Kappenman, John. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*. Goleta, CA: Metatech, January 2010. https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf.

"Key Players." NERC (North American Electric Reliability Corporation). n.d. https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx.

Kissane, Carolyn, and Emily Medina. "Energy Aftershocks in Store after Seismic Mexican Election." *The Hill*, July 3, 2018. http://thehill.com/opinion/energy-environment/395383-energy-aftershocks-in-store-after-seismic-mexican-election.

Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO*. Washington, DC: Atlantic Council, May 2016. http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf.

Lawrence, Bill, Charlotte de Seibert, and Philip Daigle. "E-ISAC Update." Presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, FL, March 6–7, 2018. https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf.

Lazar, Jim. *Electricity Regulation in the US: A Guide*. 2nd ed. Montpelier, VT: Regulatory Assistance Project, June 2016. http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf.

Lewis, James A. "North Korea and Cyber Catastrophe—Don't Hold Your Breath." *38 North*, January 12, 2018. http://www.38north.org/2018/01/jalewis011218/.

———. *Rethinking Cybersecurity: Strategy, Mass Effect, and States.* Washington, DC: CSIS, January 2018. http://espas.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf.

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf.

Lucas, Todd. "Conservative Operations." Presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, CO, September 18–19, 2013. http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf.

Lynch, Justin. "How the Russian Government Allegedly Attacks the American Electric Grid." *Fifth Domain*, July 24, 2018. https://www.fifthdomain.com/critical-infrastructure/2018/07/24/how-the-russian-government-attacks-the-american-electric-grid/.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sept./Oct. 2010). https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

"Maritime Forces Pacific." Royal Canadian Navy. Last modified November 24, 2016. http://www.navy-marine.forces.gc.ca/en/about/structure-marpac-home.page.

Marks, Joseph. "DHS Stands up New Cyber Risk Center to Protect High-Value Targets." *Nextgov*, July 31, 2018. https://www.nextgov.com/cybersecurity/2018/07/dhs-stands-new-cyber-risk-center-protect-high-value-targets/150179/.

Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Reston, VA: Noblis, January 12, 2017. http://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf.

McElwee, Steven. "Probabilistic Cluster Ensemble Evaluation for Unsupervised Intrusion Detection." Unpublished thesis, Nova Southeastern University, forthcoming.

McElwee, Steven, Jeffrey Heaton, James Fraley, and James Cannady. "Deep Learning for Prioritizing and Responding to Intrusion Detection Alerts." In *2017 IEEE Military Communications Conference Proceedings*. Piscataway, NJ: IEEE, 2017. https://ieeexplore.ieee.org/document/8170757/.

McGhee, Michael. "EEI Executive Advisory Committee." Slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017. http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf.

Miller, James N. "Cyber Deterrence Cannot Be One Size Fits All." *Cipher Brief*, August 3, 2017. https://www.thecipherbrief.com/column_article/cyber-deterrence-cannot-be-one-size-fits-all-1092.

Miller, James N., and James R. Gosler. "Memorandum for the Chairman, Defense Science Board" (preamble). In *Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf.

Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: CNAS, September 2017. https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Project Pathways-Finalb.pdf?mtime=20170918101505.

Miller, Rich. "Con Edison Shuts off Power in Lower Manhattan." *DataCenter Knowledge*, October 29, 2012. http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutown.

MISO (Midcontinent Independent System Operator). *Geomagnetic Disturbance Operations Plan*. SO-P-AOP-01 Rev: 1. Carmel, IN: MISO, June 9, 2017. https://old.misoenergy.org/_layouts/miso/ecm/redirect.aspx?id=252214.

———. "MISO January 17–18 Maximum Generation Event Overview." Slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018. https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf.

Mitchell, A. Weiss. "The Case for Deterrence by Denial." *American Interest*, August 12, 2015. https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/.

"M-1 Reserve Margin." NERC (North American Electric Reliability Corporation). n.d. https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx.

Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, September 12, 2014. http://www.38north.org/2014/09/emurauskaite091214/.

Nakashima, Ellen. "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks." *Washington Post*, July 8, 2017. https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html.

NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity: A Primer for State Utility Regulators*. Version 3.0. Washington, DC: NARUC, January 2017. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

———. *Resolution on Physical Security*. Washington, DC: NARUC, July 16, 2014. https://pubs.naruc.org/pub.cfm?id=53A0CAA5-2354-D714-5127-E0C411BAD460.

NASEO (National Association of State Energy Officials). "Comments of the National Association of State Energy Officials." In *Response to RIN 1901–AB40*. https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901%E2%80%93ab40.pdf.

NATF (North American Transmission Forum). *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Charlotte, NC: NATF, 2017. http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf.

———. *North American Transmission Forum External Newsletter*. Charlotte, NC: NATF, January 2018. https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf.

National Defense Authorization Act for Fiscal Year 2017. Public Law 114-328. *U.S. Statutes at Large* 130 (2016): 2685–2687. https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf.

NERC (North American Electric Reliability Corporation). *BAL-002-2(i)—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Washington, DC: NERC, January 1, 2018. https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf.

———. *CIP-014-2—Physical Security*. Washington, DC: NERC, October 2, 2015. http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf.

———. *EOP-010-1—Geomagnetic Disturbance Operations*. Washington, DC: NERC, June 2014. http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States.

———. *EOP-011-1—Emergency Operations*. Washington, DC: NERC, April 1, 2017. https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States.

———. *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: NERC, last updated July 3, 2018. https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

———. *Grid Security Exercise: GridEx III Report*. Atlanta, GA: NERC, March 2016. https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.

———. *Grid Security Exercise GridEx IV: Lessons Learned*. Atlanta, GA: NERC, March 28, 2018. https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf.

———. *History of NERC*. Washington, DC: NERC, August 2013. http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf.

———. *Hurricane Harvey Event Analysis Report*. Washington, DC: NERC, March 2018. https://www.nerc.com/pa/rrm/ea/Hurricane_Harvey_EAR_DL/NERC_Hurricane_Harvey_EAR_20180309.pdf.

———. "Informational Filing on the Definition of 'Adequate Level of Reliability.'" Filing to the Federal Energy Regulatory Commission. May 10, 2013. https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf.

———. *IRO-008-2—Reliability Coordinator Operational Analysis and Real-Time Assessments*. Washington, DC: NERC, April 1, 2017. https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-008-2.pdf.

———. *PRC-010-2—Under Voltage Load Shedding*. Washington, DC: NERC, April 2, 2017. http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States.

———. *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*. Atlanta, GA: NERC, December 13, 2017. https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Gas_and_Electrical_Operational_Coordination_Considerations_20171213.pdf.

———. *Reliability Terminology*. Atlanta, GA: NERC, August 2013. https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf.

———. *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*. Atlanta, GA: NERC, May 2016. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf.

———. *Standard PRC-006-3—Automatic Underfrequency Load Shedding*. Washington, DC: NERC, October 1, 2017. http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States.

———. *Technical Report Supporting Definition of Adequate Level of Reliability*. Washington, DC: NERC, March 26, 2013. https://www.nerc.com/comm/Other/Pages/Adequate%20Level%20of%20Reliability%20Task%20Force%20ALRTF.aspx.

———. *TOP-001-3—Transmission Operations*. Washington, DC: NERC, April 1, 2017. https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-3.pdf.

———. *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. Washington, DC: NERC, December 2014. http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States.

———. *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System*. Atlanta, GA: NERC, May 2013. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.

———. *2016 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2016. https://www.nerc.com/pa/rapa/ra/reliability%20assessments%20dl/2016%20long-term%20reliability%20assessment.pdf.

———. *VAR-001-4.2—Voltage and Reactive Control*. Washington, DC: NERC, September 2017. https://www.nerc.com/pa/Stand/Reliability%20Standards/VAR-001-4.2.pdf.

NERC (North American Electric Reliability Corporation) Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Princeton, NJ: NERC, July 13, 2014. https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf.

NERC (North American Electric Reliability Corporation) System Protection and Control Subcommittee. *Reliability Fundamentals of System Protection*. Princeton, NJ: NERC, December 2010. https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals_Approved_20101208.pdf.

NETL (National Energy Technology Laboratory). *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units—Volume I: The Critical Role of Thermal Units during Extreme Weather Events*. Washington, DC: DOE, March 13, 2018. https://www.netl.doe.gov/research/energy-analysis/search-publications/vuedetails?id=2594.

Newman, Lily Hay. "Hacker Lexicon: What Is the Attribution Problem?" *Wired*, December 24, 2016. https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/.

NIAC (National Infrastructure Advisory Council). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: NIAC, August 2017. https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

Nielsen, Kirstjen M. "National Cybersecurity Summit Keynote Speech." DHS (Department of Homeland Security). Released July 31, 2018. https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech.

"NOAA Space Weather Scales." NOAA. April 2011. https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf.

"North America." NERC (North American Electric Reliability Corporation). n.d. https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx.

"The North Atlantic Treaty." North Atlantic Treaty Organization. April 4, 1949 (as amended). https://www.nato.int/cps/ic/natohq/official_texts_17120.htm.

Nye, Joseph S., Jr. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (Winter 2016/2017): 44–71. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.

Obama, Barack. *Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions*. Washington, DC: The White House, July 6, 2012. https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-.

———. *Executive Order—Coordinating Efforts to Prepare the Nation for Space Weather Events*. Washington, DC: The White House, October 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events.

———. *Executive Order—Improving Critical Infrastructure Cybersecurity*. Executive Order 13636. Washington, DC: The White House, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

———. *Executive Order—National Defense Resources Preparedness*. Washington, DC: The White House, March 16, 2012. https://obamawhitehouse.archives.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness.

———. *United States Cyber Incident Coordination*. Presidential Policy Directive 41. Washington, DC: The White House: July 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

ODNI (Office of the Director of National Intelligence). *A Common Threat Framework: A Foundation for Communication*. McLean, VA: ODNI, January 26, 2018.

Orenstein, Daniel G., and Lexi C. White. *Emergency Declaration Authorities across All States and D.C.* Edina, MN: Network for Public Health Law, June 16, 2015. https://www.networkforphl.org/_asset/gxrdwm/Emergency-Declaration-Authorities.pdf.

Paradise, Theodore J., et al. "ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance–RIN 1901–AB40." Email to Jeffrey Baumgartner, US Department of Energy, February 6, 2017. http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf.

Parfomak, Paul W. *Pipelines: Securing the Veins of the American Economy, Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*. Washington, DC: Congressional Research Service, April 19, 2016. http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf.

Parfomak, Paul W., Richard J. Campbell, Robert Pirog, Michael Ratner, Phillip Brown, John Frittelli, and Marc Humphries. *Cross-Border Energy Trade in North America: Present and Potential*. Washington, DC: Congressional Research Service, January 30, 2017. https://fas.org/sgp/crs/misc/R44747.pdf.

Perry, Richard (US secretary of energy). Letter to the Federal Energy Regulatory Commission. September 28, 2017. https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf.

Phillips, Tony. "Solar Shield—Protecting the North American Power Grid." *NASA Science*, October 26, 2010. https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield.

PJM. "Comments and Responses of PJM Interconnection, L.L.C." In *Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000). March 9, 2018. http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx.

———. "Conservative Operations." Training materials presented on January 27, 2015. https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en.

———. *PJM Manual 13: Emergency Operations*. Rev. 65. Audubon, PA: PJM, January 1, 2018. http://www.pjm.com/~/media/documents/manuals/m13.ashx.

Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." *National Guard*, September 19, 2017. http://www.nationalguard.mil/News/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/.

Reagan, Ronald. "The President's News Conference." August 12, 1986. Transcript. The American Presidency Project, Gerhard Peters and John T. Woolley. http://www.presidency.ucsb.edu/ws/?pid=37733.

"Reliability Coordinators." NERC (North American Electric Reliability Corporation). As of June 1, 2015. https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx.

"REMEDYS: Research Exploring Malware in Energy Delivery Systems." Cyber Resilient Energy Delivery Consortium. March 26, 2018. https://cred-c.org/researchactivity/remedys-research-exploring-malware-energy-delivery-systems.

"The Role of Microgrids in Helping to Advance the Nation's Energy System." DOE (US Department of Energy). n.d. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping.

"Roles and Responsibilities of Governments in Natural Resources." Natural Resources Canada. Last modified October 2, 2017. http://www.nrcan.gc.ca/mining-materials/taxation/8882.

Rosenbach, Eric. "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks." *Prepared Statement for the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. June 12, 2017. https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf.

"Sandia's Grid Modernization Program Newsletter." Sandia National Laboratories. December 2017. https://content.govdelivery.com/accounts/USDOESNLEC/bulletins/1c11ce6.

Schwartz, Ian. "Sen. Tillis: We Are Living in a Glass House Throwing Rocks Complaining about Election Interference." *RealClear Politics*, January 5, 2017. https://www.realclearpolitics.com/video/2017/01/05/sen_tillis_we_are_living_in_a_glass_house_throwing_rocks_complaining_about_election_interference.html.

"Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." DOE (Department of Energy). February 14, 2018. https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency.

SERC. *Conservative Operations Guidelines*. Guide-800-101. Charlotte, NC: SERC, May 20, 2015. https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2.

Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations*. Washington, DC: NERC, May 9, 2012. https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

Shelton, William L. "Threats to Space Assets and Implications for Homeland Security." *Written Testimony before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*. March 29, 2017. http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf.

Sistrunk, Chris. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." *SANS Industrial Control Systems Security Blog*, January 8, 2016. https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one.

Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (Winter 2016/17): 73–109. https://www.mitpressjournals.org/doi/10.1162/ISEC_a_00267.

Smith, Rebecca. "U.S. Officials Push New Penalties for Hackers of Electrical Grid." *Wall Street Journal*, August 5, 2018. https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714.

Smith, Scott S. "Roles and Responsibilities for Defending the Nation from Cyber Attack." *Testimony Before the Senate Armed Services Committee*. October 19, 2017. https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities.

Sobczak, Blake, Hannah Northey, and Peter Behr. "Cyber Raises Threat against America's Energy Backbone." *Energy Wire*, May 23, 2017. https://www.eenews.net/stories/1060054924/.

Social Media Working Group for Emergency Services and Disaster Management. *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf.

"Spare Transformers." EEI (Edison Electric Institute). n.d. http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

Stanley, Andrew J. *Mapping the U.S.-Canada Energy Relationship*. Washington, DC: CSIS, May 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_Stanley_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz.

"State and Local Energy Assurance Planning." DOE (US Department of Energy). n.d. https://www.energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning.

State of New Jersey Board of Public Utilities. *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196). March 18, 2016. http://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf.

Stockton, Paul. On behalf of Exelon Corporation. *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*. Docket No. RM18-1-000. October 23, 2017.

———. "Thresholds and Criteria for Declaring Grid Security Emergencies." Study for the US Department of Energy. January 31, 2018.

Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare* (blog), July 4, 2017. https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

"Transmission Equipment Ready When Needed." Grid Assurance. n.d. http://www.gridassurance.com/equipment-subscribers/.

Trump, Donald. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Executive Order 13800. Washington, DC: The White House, May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." *ACM Transactions on the Web* 1, no. 1 (October 2017): 1:1–1:34. https://pdfs.semanticscholar.org/d310/47e426b8b5c2aa52108899a800bedd966f07.pdf.

"United States Mandatory Standards Subject to Enforcement." NERC. n.d. https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States.

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: DOE, April 2004. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

US Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: US Cyber Command, released March 2018. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.

Van Broekhoven, S. B., N. Judson, S. V. T. Nguyen, and W. D. Ross. *Microgrid Study: Energy Security for DoD Installations*. Technical Report 1164. Lexington, MA: MIT, June 2012. https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf.

Vine, Doug. *Interconnected: Canadian and U.S. Electricity*. Arlington, VA: Center for Climate and Energy Solutions, March 2017. https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf.

Walker, Bruce J. *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources*. March 1, 2018. https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1.

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

Western Electricity Coordinating Council. "Conservative System Operations." Training slides. n.d. http://docplayer.net/55224883-Conservative-system-operations.html.

The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

"Work Continues on ITC Lake Erie Project." *Transmission Hub,* February 19, 2018. https://www.transmissionhub.com/articles/2018/02/work-continues-on-itc-lake-erie-project.html.

Acknowledgments

My special thanks go to Robert Denaburg, senior analyst at Sonecon LLC. I also thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Wayne Austad (Idaho National Laboratory); Terry Boston; Stuart Brindley; Gerry Cauley; Richard Danzig (JHU/APL); Daniel Elmore (Idaho National Laboratory); Peter Grandgeorge (Berkshire Hathaway Energy); Emily Goldman (US Cyber Command); Sean Griffin (ecubed us LLC); Dave Halla (JHU/APL); Jon Jipping (ITC Holdings); Debra Lavoy (Narrative Builders); Bill Lawrence (NERC); Joseph Maurio (JHU/APL); James Miller (JHU/APL); Michael Moskowitz (JHU/APL); Richard Mroz; Steven T. Naumann (Exelon Corporation); Catherine Peacock (JHU/APL); Emilia Probasco (JHU/APL); Erin Richardson (JHU/APL); David Roop (Dominion Energy); Matthew Schaffer (JHU/APL); senior leaders at Southern Company; Kyle Thomas (Dominion Virginia Power); and Virginia Wright (Idaho National Laboratory). I also thank the many additional industry and government reviewers who preferred to remain anonymous.

About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of JHU/APL. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support in Superstorm Sandy and other disasters. Dr. Stockton also served as the Department of Defense (DOD) domestic crisis manager and was responsible for defense critical infrastructure protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere. 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, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, MD: JHU/APL, 2016) and numerous other publications. He served as the facilitator of the GridEx IV exercise (November 2017) and is a member of the Homeland Security Advisory Council and other public and private sector boards.

APL

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY