SUPERSTORM SANDY: IMPLICATIONS FOR DESIGNING A POST-CYBER ATTACK POWER RESTORATION SYSTEM

National Security Perspective

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

SUPERSTORM SANDY: IMPLICATIONS FOR DESIGNING A POST-CYBER ATTACK POWER RESTORATION SYSTEM

Paul 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 Homeland Security or any other US government agency or of JHU/APL sponsors.

NSAD-R-15-075

Contents

Abstract

Sophisticated cyber attacks on the electric grid will create power restoration challenges starkly different from those in Superstorm Sandy or other previous outages in the United States. Nevertheless, rather than build a separate restoration system for cyber events, electric utilities and their government partners should explore how they can leverage existing mutual assistance agreements and other mechanisms to meet the challenges of the cyber era.

This study summarizes restoration challenges posed by Sandy and contrasts them with those that would be produced by a cyber attack on the grid. The study then examines the implications of these disparate challenges for the electricity industry's mutual assistance system and proposes potential steps to build an "all-hazards" system that can account for the unique problems that cyber attacks will create. The study also analyzes support missions that state and federal agencies might perform in response to requests for assistance from utilities and analyzes how to build a cyber response framework that can coordinate such requests. The study concludes by examining how utilities might prepare in advance for post-cyber attack opportunities to strengthen the architecture of the grid in ways that are not politically or economically feasible today.

Executive Summary

The electric power industry and its public sector partners are rising to meet a new challenge in cyber resilience. Thus far, their efforts have concentrated on protecting the grid and making it less susceptible to attack. Those efforts are vital and must continue. However, given the increasing severity of the cyber threat, utilities and their partners must also accelerate progress in another dimension of resilience: improving plans, capabilities, and coordination mechanisms to restore power and reestablish the integrity of grid control systems if cyber defenses fail.

This study discusses opportunities to accelerate power restoration after a sophisticated cyber attack on the US grid. As a starting point, the study examines how utilities restored power so effectively after Superstorm Sandy and analyzes the problems that utilities confront in building an equivalent restoration system to respond to sophisticated cyber threats. The study also examines the starkly different requests for government support for restoration that might result from a cyber attack. In addition, the study derives lessons learned from Sandy for coordinating such assistance so that it actually serves utilities' priorities—as opposed to being in the way.

After Sandy, power was restored remarkably quickly because so many utilities across the United States pitched in to help. State and federal agencies aided this flow by responding to industry requests for transportation aircraft and other support capabilities. An equivalent restoration system, tailored to meet the challenges of cyber attacks rather than storms, is essential to build resilience against potential adversaries who are aggressively mapping the US power grid and hiding malware within it.

However, adapting the current restoration system for post-cyber attack operations will entail major challenges. During Sandy, utilities sending assistance to the impact zone were secure in the knowledge that they were safely beyond the reach of the storm. No power company will be beyond harm's way during a nationwide cyber attack. To help restore power when many utility chief executive officers (CEOs) will worry that their companies are next in line for attack, mutual assistance agreements may need to overcome powerful disincentives to provide scarce restoration capabilities. Utilities can leverage exercises such as GridEx to develop specialized agreements and support protocols that can meet these challenges, just as they are doing now for coordinated physical attacks on the grid and other man-made threats.

Differences among the industrial control systems (ICSs) utilities use to manage their operations pose an additional problem. During Sandy, restoration crews arriving from the West Coast could directly contribute to repair efforts of Consolidated Edison and other companies in the stricken region because restringing power lines and other restoration tasks are similar from one utility to the next. Much greater variation exists across ICS software, applications, and system designs. Restoring these operational technology (OT) systems after a cyber attack requires specialized utility-specific training. The electricity sector and its contractors might want to explore cross utility pilot programs to determine how best to overcome these training challenges and whether such programs might be scaled up to help meet regional restoration needs. The sector might assess whether existing standards and interoperability initiatives are sufficient to mitigate the cross utility challenges that would be presented by restoration tasks. The sector might also identify which restoration tasks can be performed with less specialized knowledge so that it can focus cyber mutual assistance on providing those functions, allowing more highly trained personnel in a stricken utility to concentrate on ICS remediation.

The utility-specific nature of these OT systems will also limit the ability of government agencies to assist power restoration. State National Guard units offer the most promising potential source of support. Guard personnel performed crucial road clearance and other operations to assist grid repair crews after Sandy. Now, a growing number of State Guard

organizations and Department of Defense (DOD) contractors are partnering with their local utilities to train personnel to support post-cyber attack power restoration. These efforts should be evaluated for their cost effectiveness to determine whether they can be expanded nationwide.

Whether US Cyber Command (USCYBERCOM) should be structured to augment this support is less clear. The command has a growing cadre of cyber protection teams with ICS remediation skills. However, these teams' primary focus in an attack will be to protect DOD networks and functions. As occurred during Sandy, the president could direct the DOD to make power restoration a top priority, especially when defense networks remain secure and cyber protection assets are readily available for support missions. Yet, the authorities under which USCYBERCOM would help utilities remediate their OT systems remain uncertain, as do the specific functions that utilities would want USCYBERCOM to perform. Cyber Guard and other exercises could examine and further clarify whether and how USCYBERCOM might assist such power restoration operations.

Restoration after Sandy benefited from a strong foundation to coordinate federal assistance to states and their utilities, undergirded by the *National Response Framework* (NRF). The equivalent document for the cyber realm—the interim *National Cyber Incident Response Plan* (2010)—would almost surely prove inadequate just when the United States needed it most. An especially critical shortfall of the interim plan: it provides state governors with only a minimal role in guiding cyber response efforts, even though state National Guard organizations will likely play an increasingly significant role in supporting power restoration and other response operations. The core principles of the NRF (including its reliance on governors) should be leveraged to build a new national framework for cyber response, including an effective process for requesting assistance. The cyber response framework should complement and be integrated with other public and private sector initiatives to strengthen power restoration capabilities, especially the playbook initiative led by the Electricity Subsector Coordinating Council (ESCC). The framework should also account for cyber response tasks that go beyond those required for natural hazards, including attributing a cyber attack to those responsible for launching it.

The electricity subsector and its partners should also explore how the grid might be reconstituted once utilities have completed initial power restoration operations in an event. A cyber attack that successfully disrupts subsector functions and services may open the door to changes in the grid architecture that are too technically difficult, expensive, or politically impractical to adopt today. In addition to aggressively accelerating current efforts to strengthen grid resilience, utilities and their partners should begin developing options to reconstitute the post-attack grid before an attack occurs, so that these options will be readily available in the new political and resilience funding environment that a major outage could create.

The first section of this study summarizes restoration challenges posed by Sandy and contrasts them with those that would be created by a sophisticated cyber attack on the grid. The second section examines the implications of these disparate challenges for the electricity industry's mutual assistance system and proposes potential steps to build an "all-hazards" system that can account for the unique problems that cyber attacks will create. The third section analyzes support missions that state and federal agencies might perform in response to requests for assistance (RFAs) from utilities. The fourth section analyzes how to build a cyber response framework that can coordinate RFAs and help integrate power restoration support. Finally, the fifth section examines the phasing of power restoration efforts over the longer term, including post-cyber attack opportunities to strengthen the architecture of the grid in ways that are not politically or economically feasible today.

The Power Restoration Challenge

Lessons Learned from Superstorm Sandy

Sandy packed a one-two punch for electric infrastructure. On the night of October 29, 2012, Sandy made landfall near Atlantic City, New Jersey, as a post-tropical cyclone. Over the next three days, the impacts of Sandy could be felt from North Carolina to Maine and as far west as Illinois. With an unprecedented storm surge in the affected areas, there was especially severe damage to the energy infrastructure. Peak outages to electric power customers occurred on October 30 and 31 as the storm proceeded inland from the coast, with peak outages in all states totaling over 8.5 million, as reported in the Department of Energy (DOE) Situation Reports. Much of the damage was concentrated in New York and New Jersey, with some customer outages and fuel disruptions lasting weeks.[1] The second punch landed on November 7, 2012, as a nor'easter impacted the Mid-Atlantic and Northeast with strong winds, rain and snow, and coastal flooding. The second storm caused power outages for more than 150,000 additional customers and prolonged recovery.[2]

The combined damage to critical electricity substations, high-voltage transmission lines, and other key grid components was massive—as would be expected from the second-largest Atlantic storm on record.[3] Some major utilities in the region suffered from gaps in their preparedness to conduct repair operations on the scale that Sandy required.[4] Overall, however, utilities restored power with remarkable speed and effectiveness in most areas hit by the superstorm. Despite the vast number of grid components that needed to be repaired or replaced and the fallen trees and other impediments that restoration crews encountered, within two weeks of Sandy's landfall, utilities had restored power to 99 percent of customers who could receive power.[5]

The mutual assistance system in the electric industry was the linchpin for this success. Although the linemen and other power restoration personnel in utilities across Sandy's impact zone performed admirably, no single utility retains the restoration capabilities needed to repair the damage caused by a storm on that scale. Achieving such restoration preparedness would be extraordinarily expensive. Moreover, given the rarity of such catastrophic events, the amount of money required to enable a utility to restore power on its own would be difficult to justify as a prudent expense to state public utility commissions (PUCs), shareholders, or elected officials responsible for approving such expenditures.[6] Instead, utilities have built a highly effective voluntary system of

[1] US Department of Energy, Office of Electricity Delivery and Energy Reliability, *Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement* (Washington, DC: US Department of Energy, February 26, 2013), 2, http://energy.gov/sites/prod/files/2013/05/f0/DOE_Overview_Response-Sandy-Noreaster_Final.pdf.

[2] Ibid., 4.

[3] US Federal Emergency Management Agency (FEMA), *Hurricane Sandy FEMA After-Action Report* (Washington, DC: US Federal Emergency Management Agency, July 1, 2013), 4, https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf.

[4] The Moreland Commission to Investigate Public Corruption, *Moreland Commission Report on Utility Storm Preparation and Response: Final Report* (New York: Moreland Commission, June 22, 2013), http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/MACfinalreportjune22.pdf; and Danny Hakim, Patrick McGeehan, and Michael Moss, "Suffering on Long Island as Power Agency Shows Its Flaws," *New York Times*, November 13, 2012, http://www.nytimes.com/2012/11/14/nyregion/long-island-power-authoritys-flaws-hindered-recovery-efforts.html?_r=0.

[5] US Department of Energy, *Overview*, 4. For a detailed breakdown of restoration time lines, see Rae Zimmerman, "Planning Restoration of Vital Infrastructure Services following Hurricane Sandy: Lessons Learned for Energy and Transportation," *Journal of Extreme Events* 1, no. 1 (2014): 1450004-1–1450004-38.

[6] On cost recovery constraints associated with investments in power system resilience and restoration operations, including labor force levels and standby equipment, see Edison Electric Institute, *Before and after the Storm: A Compilation of Recent Studies, Programs, and Policies Related to Storm Hardening and Resiliency, Update* (Washington, DC: Edison Electric Institute, March 2014), 13–15 and 19–26, http://www.eei.org/

mutual support, whereby utilities that are not at risk of being struck by a hurricane or other hazard can send restoration assets to those that are. The overall restoration capacity of the industry is immense; the mutual assistance system enables utilities to target support when and where specific utilities request aid.

Sandy highlighted the effectiveness of this system. Tens of thousands of mutual assistance personnel, including linemen, engineers, vegetation crews, and support personnel provided by eighty electric utilities from across the United States, flowed in to the area to help the utilities hit by Sandy—by far the largest deployment of mutual assistance capabilities in US history.[7] Utilities contributed these assets from the West Coast, the Midwest, and other regions far beyond the storm's footprint. Now, drawing on the lessons learned from Sandy, utilities are expanding the mutual assistance system to bring to bear still greater restoration capabilities in future catastrophes.[8]

This system did not emerge by chance. For decades, hurricanes and other severe weather events have hammered utilities in the eastern and southern United States. Massive ice storms, wildfires, and other natural hazards have also inflicted wide-area power outages in other regions of the United States. In response, utilities gradually built up the mutual assistance system, developing increasingly effective governance and decision-making mechanisms to allocate restoration crews and other limited resources and prioritize assistance when multiple power providers requested help.[9] Restoration crews have become as expert at line stringing, replacing power poles, and performing other functions for partner utilities as they are for their own organizations. So that personnel stay sharp between events, utilities conduct frequent exercises that are modeled on the hurricanes and other hazards they typically face. They have also established mechanisms to reimburse each other for the cost of providing assistance and (together with state PUCs) have created special cost recovery mechanisms to help pay for restoration operations in severe storms.

Decades of experience also strengthened government support for power restoration after Sandy. When the superstorm hit, state National Guard personnel in New York, New Jersey, and other states were already prepared to perform well-established (and crucial) support functions at the request of their local utilities, including road clearance and debris removal to help utility repair crews reach damaged equipment. The Emergency Management Assistance Compact (EMAC) system enabled thirty-seven states outside the affected area to send thousands of additional Guard personnel to help to execute these missions.[10] The *National Response Framework* (NRF) also provided time-tested mechanisms to coordinate the provision of government assistance.[11] Moreover, as in the case of the power industry's mutual assistance system, federal and state agencies have launched a wide array of initiatives to draw on lessons learned from the superstorm and strengthen support for power restoration in future catastrophic blackouts.

The key underlying factors that made power restoration so effective after Sandy are absent in the cyber realm. Utilities and state National Guard organizations outside of the storm's track were able to send their own restoration assets to the affected area safe in the knowledge that their own states would

issuesandpolicy/electricreliability/mutualassistance/Documents/BeforeandAftertheStorm.pdf.

[7] FEMA, *Hurricane Sandy FEMA After-Action Report*, 4.

[8] Edison Electric Institute, *Before and after the Storm*, Appendix C.

[9] B. Jim Reagan, "Mutual Assistance: Changing a Paradigm?" (talk presented at California Utilities Emergency Association Annual Meeting, San Diego, CA, June 6, 2013), www.cueainc.com/documents/Mutual%20Assistance.pptx.

[10] "The EMAC Response to Hurricane Sandy," National Emergency Management Association, accessed January 13, 2016, http://www.nemaweb.org/index.php/54-em-advocate/emac-news-archive/566-the-emac-response-to-hurricane-sandy.

[11] US Department of Homeland Security, *National Response Framework*, 2nd ed. (Washington, DC: US Department of Homeland Security, May 2013), https://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

not be hit. In contrast, cyber adversaries may be able to launch attacks nationwide. During Sandy, repair crews from outside the affected area were able to help the affected utilities because wire stringing and other missions are substantially similar from company to company. Industrial control systems (ICSs) and other potential cyber attack targets differ widely among utilities and often require detailed system-specific knowledge to repair.

Moreover, decades of experience with hurricanes and other natural hazards shaped the power restoration system for events such as Sandy. Cyber attacks have yet to take down regional US power systems or provide any comparable real-world experience to drive the design of a cyber-oriented system. Utilities face near-constant cyber penetration efforts, including attempts to break into their ICSs and other operational technology (OT) networks that help monitor and control the grid. But cyber weapons that destroy or disrupt grid components will present real-world power restoration challenges that have never been experienced in the United States and whose requirements differ markedly from those that the current restoration system has been optimized to meet.

Utilities and their partners will need to anticipate the restoration requirements that emerging cyber threats to the grid will create. In particular, they will need to develop a design basis to help size and structure the response system for post-attack power restoration, and they will need to adapt mutual assistance agreements, government support missions, and coordination mechanisms that the United States will require to respond to increasingly capable cyber adversaries.

Setting a Design Basis for the Restoration System

Admiral Michael Rogers, the combatant commander of US Cyber Command (USCYBERCOM), notes, "We have seen nation states spending a lot of time and a lot of effort to try to gain access to the [electric] power structure within the United States," as well as to other critical infrastructure. Admiral Rogers concludes that these nations are doing so "to generate options and capabilities for themselves should they decide that they want to potentially do something."[12]

However, ongoing efforts to map utility control networks and hide malware on them provide only a starting point to assess requirements for power restoration. The BlackEnergy campaign illustrates both the value and the limitations of using current cyber penetration activities to help size and structure the restoration system. In 2014, the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned utilities that this sophisticated malware "has compromised numerous . . . ICSs" and that "multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs)."[13]

ICS-CERT reported that it has not been able to verify whether the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, the alert noted that "typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment."[14]

BlackEnergy highlights the effectiveness of current adversaries' efforts to establish a presence in utility ICSs and the difficulty of determining how far the malware has spread across key networks and control

[12] Damian Paletta, "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent," *Wall Street Journal*, September 8, 2015, http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541.

[13] "Alert (ICS-ALERT-14-281-01B): Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," Industrial Control Systems Cyber Emergency Response Team, original release date December 10, 2014, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[14] Ibid.

mechanisms.[15] Indeed, simply detecting the presence of such sophisticated malware poses a major challenge: ICS-CERT notes that the BlackEnergy campaign has been under way against US infrastructure since 2011 or even earlier.[16] Havex and other difficult-to-detect advanced persistent threats (APTs) further illustrate the growing effectiveness of both malware payloads and the attacker's access strategies, including phishing e-mails, redirections to compromised websites, and trojanized update installers on ICS vendor websites (i.e., "watering-hole" attacks).[17]

However, while such network reconnaissance and APT campaigns can help "prepare the battlefield" for subsequent attacks on the grid, potential adversaries are unlikely to reveal the most effective weapons they have in their cyber arsenals until they use them. In a crisis, these adversaries could conceivably want to prove to US leaders that they hold the power grid at risk. More typically, however, adversaries can be expected to hold their most disruptive weapons in reserve until launching an attack, thereby reducing the risk that the United States can build and deploy defenses against them.

It will also be important to size and structure the proposed power restoration system to account for the growing severity of the threat. It will take years to establish such a system, develop the governance mechanisms it requires, and train and exercise OT teams so they can effectively function in the stressful operational circumstances that cyber warfare will create. Limited budgets, combined with the difficulty of implementing such changes, will make this an incremental process. Nevertheless, to build consensus on the design requirements that such a system should ultimately achieve, it is essential to anticipate the restoration challenge that utilities will confront in 2020 and beyond.

Accounting for Uncertainties in Future Restoration Requirements

Utilities and their partners will need to overcome three problems to reach consensus on this design basis. The first is the difficulty of knowing how adversaries' capabilities will grow. Director of National Intelligence James Clapper, Deputy Secretary of Defense Robert Work, and other senior national security officials emphasize that the grid and other US critical infrastructure targets face increasingly sophisticated and potentially disruptive cyber threats.[18] The number of potential adversaries with access to such advanced capabilities is also climbing. Secretary Work notes:

> To conduct a disruptive or destructive cyber operation against a military or industrial control system requires expertise, but a potential adversary need not spend millions of dollars to develop an offensive capability. A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities through the online marketplaces created by cyber criminals, or through other black markets. As cyber capabilities become more readily available over time, the Department of Defense

[15] Lucian Constantin, "Attack Campaign Infects Industrial Control Systems with BlackEnergy Malware," *PCWorld*, October 29, 2014, http://www.pcworld.com/article/2840612/attack-campaign-infects-industrial-control-systems-with-blackenergy-malware.html.

[16] "Alert (ICS-ALERT-14-281-01B)."

[17] "Advisory (ICSA-14-178-01): ICS-Focused Malware," Industrial Control Systems Cyber Emergency Response Team, original release date July 01, 2014, https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01; and *ICS-CERT Monitor*, May/June 2015 issue, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

[18] *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong. (September 29, 2015) (statement of James R. Clapper, Director of National Intelligence), http://www.armed-services.senate.gov/imo/media/doc/Clapper_09-29-15.pdf; and *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong. (September 29, 2015) (statement of Robert O. Work, Deputy Secretary of Defense), http://www.armed-services.senate.gov/imo/media/doc/Work_09-29-15.pdf.

> assesses that state and non-state actors will continue to seek and develop malicious cyber capabilities to use against U.S. interests.[19]

To account for the geographic scale and scope of the blackouts such actors will be able to inflict in 2020 and beyond, and to build consensus on how the power restoration system should be sized accordingly, the federal government must continue to strengthen its information sharing with cleared industry personnel on the nature of the emerging threat. It will also be critical to facilitate the flow of information on threat signatures and other data from industry to government agencies and build on the current sharing mechanisms established by the Cyber Information Sharing and Collaboration Program and other initiatives.[20] Industry-to-industry sharing of threat information (especially in the Electricity Information Sharing and Analysis Center, or E-ISAC) will be equally essential to building the design basis for restoration. Finally, because state PUCs play a critical role in determining whether distribution companies under their jurisdictions can recover costs for investing in restoration capabilities, it will also be crucial for government agencies to help PUCs assess threat-driven requirements for investment in response capabilities. Such outreach to PUCs can succeed only if larger numbers of appropriate personnel receive security clearances.

The second challenge for establishing a design basis for the power restoration system lies in the rapid technological change under way in the US power grid and the risk that this modernization is creating unanticipated vulnerabilities to cyber attack. The integration of new digital technologies into the grid, including smart inverters and other system components that facilitate the integration of renewable generation capacity and demand response operations, is creating new "attack surfaces" for adversaries to exploit. Until utilities experience cyber warfare, it will also be difficult to assess whether the features of the grid (such as system redundancies and capabilities to reroute power) that make it so resilient against traditional hazards will limit the cascading effects of a sophisticated attack on multiple grid components, or whether the complexity of the grid will magnify the effects from such a sophisticated attack.[21]

The third challenge lies in assessing the pace and effectiveness of utility efforts to mitigate these new vulnerabilities. Utilities and their partners are acutely aware of the cyber risks that grid modernization may create and are developing innovative ways to strengthen grid security and limit cascading power failures if attacks do occur. Key initiatives being advanced by the electricity sector include the following:

- Use of "ICS Cyber Kill Chains" and other assessment methodologies to help utility OT network defenders detect and disrupt adversaries earlier in the cycle of an attack, especially against APTs[22]
- Plans and capabilities to quickly reconfigure ICSs, reset safety settings, and restore other targeted

[19] *United States Cybersecurity Policy and Threats Hearing*, Work statement, 3.

[20] US Department of Homeland Security, *Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program* (Washington, DC: US Department of Homeland Security, 2014), https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

[21] On the risks of complexiity creating cascading infrastructure failures, see Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (New York: Basic Books, 1984).

[22] Michael J. Assante 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. This work builds on the Cyber Kill Chain™ developed by Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"(paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011), www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

equipment and controls to normal (by using secured gold copy and other means)[23]

- Installation of protective relays, produced by a variety of vendors, to reduce the risks associated with relying on a single provider (although this approach introduces additional system complexity and configuration challenges)
- Initiatives to complicate the already significant challenges that adversaries face in mapping operational control networks and systems and in maintaining the accuracy and currency of those maps as utilities modify their OT systems[24]
- New technical means to detect and remove APTs from the grid systems, including firmware, and eliminate the risk of follow-on infections to replacement equipment and autonomous reattack by APTs
- Measures to retain or rapidly restore the secure, reliable data and communications essential to control the grid and reintegrate unplanned power islands in a cyber attack, even if adversaries seek to degrade Voice over Internet Protocol (VoIP) and other communications links[25]
- Steps to prevent cyber attacks from causing misoperation and physical damage to nuclear power plants, natural gas-fueled generators, and other critical grid components, thereby averting lengthy equipment restoration requirements for power restoration[26]
- Creation of more effective defenses against potential adversaries who have demonstrated the ability to compromise the product supply chains of ICS vendors, and mitigation of the risk that when downloading legitimate software updates directly from the vendors' websites, utilities will also download malware designed to facilitate exploitation[27]
- Development and deployment of power maintenance or restoration fallback systems that are invulnerable to cyber attack, including electromechanical controls (which will also require survivable communications and the retention of trained staff to maintain and operate such fallback systems)
- Creation of "last-mile" technologies or other initiatives that can create more difficult-to-bridge gaps for cyber attackers to cross[28]
- Measures to mitigate the threat of insider cyber attacks conducted by utility employees and other personnel with cleared access to networks and

[23] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advances Cyber Threat* (Washington, DC: Defense Science Board, January 2013), http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[24] Installing defenses against Shodan-enabled mapping provides a starting point for such progress. Phillip Allison, "Cloak and Secure Your Critical Infrastructure, ICS and SCADA Systems: Building Security into Your Industrial Internet" (paper presented at Pacific Northwest Section American Water Works Association Conference, Bellevue, WA, 2015), http://www.pnws-awwa.org/uploads/PDFs/conferences/2015/Technical%20Sessions/Thursday/4_Cloak%20and%20Secure%20Your%20Critical%20Infrastructure,%20ICS%20and%20SCADA%20Systems.pdf.

[25] North American Electric Reliability Corporation (NERC), Severe Impact Resilience Task Force, *Severe Impact Resilience: Considerations and Recommendations* (Washington, DC: North American Electric Reliability Corporation, 2012), 39–45, http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

[26] Jan-Ole Malchow et al., "PLC Guard: A Practical Defense against Attacks on Cyber-Physical Systems" in *Proceedings of the IEEE Conference on Communications and Network Security* (Piscataway, NJ: IEEE, 2015), 326–334.

[27] *United States Cybersecurity Policy and Threats Hearing*, Work statement.

[28] Michael Assante, Tim Roxey, and Andrew Bochman, *The Case for Simplicity in Energy Infrastructure: For Economic and National Security* (Washington, DC: Center for Strategic and International Studies, November 2015), http://csis.org/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf; and David C. Walsh, "Danzig: Analog Has Value in Countering Cyber Threats," *Defense Systems*, September 1, 2015, https://defensesystems.com/articles/2015/09/01/danzig-interview-cyber-defense.aspx.

equipment, potentially in coordination with other attack vectors[29]

- Initiatives to segment the grid if an attack occurs, preplan for islanded operations, and take other measures to prevent cascading multiregional failures of the electric system[30]
- Full implementation of the additional measures recommended by the National Institute of Standards and Technology (NIST) cybersecurity framework, the NIST updated ICS security guide, the DOE *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*, ICS-CERT reports, and other sources of guidance to drastically reduce the potential geographical scope and duration of cyber-induced blackouts

Proposed Design Basis

The North American Electric Reliability Corporation (NERC) *Cyber Attack Task Force: Final Report* (2012) provides a pioneering and technically well-informed analysis of power restoration challenges that cyber attacks would create.[31] The report sounds an important caution: while grid owners and operators "are challenged on a daily basis by new cybersecurity vulnerabilities and attempted intrusions, a successful coordinated cyber attack affecting the North American bulk power system has not yet occurred. Therefore, it is difficult to confidently determine the potential impact on the reliability of the bulk power system and what additional actions may need to be taken."[32]

Rather than make such a determination, the NERC report instead uses its analysis to propose an attack scenario that can help assess US restoration requirements. The scenario assumes that future attackers will be able to impair or disable the integrity of multiple control systems or take operating control of portions of the bulk power system such that generation or transmission systems are damaged or operated improperly. Specific attack consequences that will help drive restoration requirements include the following:

- "Transmission Operators report an unexplained and persistent breaker operation that occurs across a wide geographic area (i.e., within a state/province and neighboring state/province).
- Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
- Loss of load and generation causes widespread bulk power system instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the bulk power system remain operational.

[29] The NERC report emphasizes that "insiders pose the greatest threat, especially if they are working with a Foreign State or other High Level Threat Actors, because of their detailed knowledge of system operations and security practices. In addition, they have legitimate physical and electronic access to key systems and the controls designed to protect them. Insider individuals can provide qualitative, technical or physical assistance to the team requirements of sophisticated adversaries or pose a unique unilateral threat detection challenge, if acting alone. Individuals with the highest level of access pose the greatest threat. Furthermore, an individual with access to grid infrastructure could unwittingly or inadvertently introduce malware into a system through portable media or by falling victim to social engineering e-mails or other forms of communication." NERC, *Cyber Attack Task Force: Final Report* (Washington, DC: North American Electric Reliability Corporation, 2012), 9, http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf.

[30] NERC, *Cyber Attack Task Force*, 20–23; and NERC, *Severe Impact Resilience*, 18–39. See also NERC, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (Washington, DC: North American Electric Reliability Corporation, 2010), http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

[31] NERC, *Cyber Attack Task Force*. See NERC, *Severe Impact Resilience*, for additional details on the potential impacts of a cyber attack on the grid. See also NERC, *High-Impact, Low-Frequency Event*.

[32] NERC, *Cyber Attack Task Force*, 1.

- Blackouts in several regions disrupt electricity supply to several million people."[33]

This scenario provides a valuable point of departure to establish a design basis for the restoration system the United States should develop for 2020 and beyond. That system should be prepared to respond to attacks in multiple regions across the United States. In addition, the system should be built on the assumption that unless utilities and their partners can eliminate carefully hidden APTs from their networks, the malware will be able to reinfect replacement equipment and software and cause repeated disruptions of grid operations.

This design basis should also be refined to reflect the geopolitical circumstances in which cyber attacks are most likely to occur. Just as with nuclear weapons, the United States needs to hedge against the risk that an adversary would launch an all-out surprise cyber attack on the grid and other critical targets. However, it is much more likely that cyber attacks would occur in the context of an intensifying political crisis in the South China Sea or the Baltics or with a regional power elsewhere in the world. Deputy Secretary of Defense Robert Work notes "almost all our combat power" is now based in the United States itself. If a regional crisis emerged, and the United States launched preparations to deploy forces accordingly, "you now have to assume that you're going to be under intense cyber attack even before you move."[34]

Department of Defense (DOD) installations, networks, and private contractors needed to support these deployments could be prime targets for cyber attacks.[35] The adversary could also attack selected portions of the US grid to achieve specific political and military objectives aimed at encouraging US leaders to resolve the crisis on terms favorable to the attacker.[36] In particular, adversaries may target attacks on the grid to disrupt mission execution at key US military bases, especially those important for operations in the crisis region. Potential objectives for such targeted cyber attacks include the following:

- Degrading the ability of US defense installations to execute their critical missions by interrupting the flow of electricity to those facilities and to the water systems and other electricity-dependent infrastructure vital for defense operations
- Disabling or degrading financial systems, public health services, transportation, telecommunication nodes, and other targets that have proven to be of special concern to US elected leaders during Sandy and other blackouts
- Creating a politically tenuous situation for US leaders by demonstrating the ability to reattack the grid after initial restoration is achieved and to strike other selected power systems across the United States

A restoration system capable of restoring power in the face of these targeted attacks would be enormously helpful to US leaders during crisis management. Such a system could also serve as the foundation on which to build more extensive response capabilities sized to handle the multiregional outages envisioned by the NERC report. However, before any such buildout moves forward, it will be essential to continue to improve our technical understanding of the physical damage and other effects that cyber attacks are likely to have on the grid, including the degree to which

[33] Ibid., 2.

[34] Bradley Peniston, "Work: 'The Age of Everything Is the Era of Grand Strategy,'" *Defense One*, November 2, 2015, http://www.defenseone.com/management/2015/11/work-age-everything-era-grand-strategy/123335/.

[35] US Senate, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors: Report of the Committee on Armed Services*, 113th Cong., 2d sess., 2015, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

[36] For a broader analysis of the likelihood that adversaries will launch cyber attacks on the civilian sector to gain political leverage in a conflict, see P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 131.

adversaries can achieve cascading multiregional failures of the grid.

The analysis that follows discusses ways to build a system that can restore power after coordinated, selective attacks on US utilities during an escalating regional crisis—in other words, a targeted threat. As more data become available on adversaries' capabilities and intentions, and on the effectiveness of US efforts to reduce the vulnerability of the power grid, this preliminary design basis for the power restoration system should be revised accordingly.

Leveraging Current Mutual Assistance and Industry Restoration Systems for the Cyber Era

There are potentially significant advantages in leveraging the current mutual assistance system to meet cyber threats, rather than building a separate system for cyber threats alone. Existing sector-created systems for governance and cost reimbursement in mutual assistance operations offer particular value as a basis for progress against cyber threats. After many years of refinement and consensus building by utility chief executive officers (CEOs), power companies have developed effective decision-making mechanisms to mobilize and allocate restoration crews and other restoration assets. This governance system also enables utilities to prioritize the allocation of limited assets when multiple power providers request help. Rather than depart from this proven system, a better option would be to expand its all-hazards applicability and supplement the system with branch plans and decision-making guidelines tailored to meet cyber-specific challenges.

The analysis that follows examines four especially significant challenges and potential ways to meet them. The first problem is that cyber threats will corrode the underlying incentive structure that makes existing assistance mechanisms so effective. Second, even when utilities want to help each other, the technical challenges of restoring ICS operations (versus stringing wires after a hurricane) will limit their abilities to do so. Third, while utilities have well-understood principles and organizational practices to restore power against natural hazards, a new concept of operations (CONOPS) will be needed to guide post-cyber attack restoration operations. Fourth, who is going to pay for improvements in restoration capabilities?

Challenge 1: You Can Never Be Sure You Won't Be Hit—Repeatedly

The risk that the adversary might strike utilities nationwide would stress mutual assistance systems in ways that Sandy did not. During Sandy, governors in states beyond the storm track were able to deploy National Guard forces under EMAC, secure in the knowledge that Sandy would not hit their electric infrastructures. The same was true of utilities that provided mutual assistance under the Regional Mutual Assistance Group system (and the mutual aid programs managed by municipal and cooperative utilities) that worked so effectively during Sandy. In the assumed midrange threat, the risk that the adversary could attack utilities across the United States would create powerful incentives for governors and utility CEOs to err on the side of caution and retain restoration capabilities that their own citizens and customers might need.

The risk of reattacks would magnify these problems for mutual assistance. In a pioneering work on biological threats, Richard Danzig notes that the ability of adversaries to "reload" after an initial attack, conducting follow-on strikes using fresh supplies of the same biological agents, would put enormous stress on US response planning and preparedness against such hazards.[37] Similar challenges would emerge

[37] Richard Danzig, *Preparing for Catastrophic Bioterrorism: Toward a Long-Term Strategy for Limiting the Risk,* Defense & Technology Paper (Washington, DC: Center for Technology and National Security Policy, May 2008), http://ctnsp.dodlive.mil/files/2014/10/Preparing-for-Catastrophic-Bioterrorism.pdf.

from the ability of cyber APTs to launch reattacks on grid networks and infect replacement equipment and OT software that had been installed after the original strike. The NERC cyber report notes:

> During a cyber attack and the following aftermath, responders may be lulled into the false sense of security that there is only one wave of assault. As with a storm, once the storm passes, everyone pitches in to begin the restoration process with a clear and understood recovery plan. If the attack vector(s) and techniques/tools for the attack are not fully understood and mitigated, the attacker could launch subsequent attacks to disrupt recovery efforts or respond to mitigation efforts. These later attack waves may hold devastating impact potential if not understood and expected.[38]

Utilities will be especially reluctant to share their response capabilities with their counterparts in other regions if they will remain at risk of such devastating effects even after initial power restoration operations are complete.

These factors affect the amount of restoration capacity and support that the overall power restoration response system should be sized and structured to provide, and they help determine how scarce resources should be allocated. Utilities should also conduct exercises specially focused on the governance challenges that cyber attacks will create for the mutual assistance system. Real-world experience with hurricanes and other natural hazards has helped forge an industry consensus on how to allocate restoration resources. No such experience can help the industry prepare for the cyber attacks to come. The GridEx series and other exercises could be tailored to help CEOs drill down into the disincentives for sharing created by cyber attacks and build consensus on ways to overcome those challenges.

[38] NERC, *Cyber Attack Task Force*, 29.

Challenge 2: Capabilities for Mutual Assistance

A critical enabler for success during Sandy was that before the storm hit, utilities clearly understood the types of assistance they were likely to need and how that assistance should directly support their restoration operations. The same clarity will be essential for post-cyber attack restoration. Utility owners and operators are responsible for power restoration and have unique knowledge of their system architectures and restoration plans and challenges (including for black start operations). The risk that an adversary nation will cause a blackout in an act of war does not change that equation. On the contrary, in a cyber-induced outage, utility-specific knowledge for restoration will be *at least as vital* as in natural events such as Sandy. However, key factors that facilitate mutual assistance in events such as Sandy will be problematic in post-cyber attack power restoration.

Cross Utility Technical Expertise

Utilities have many decades of experience in executing the specific tasks required to restore service. Utility personnel have comprehensive knowledge of what it takes to erect replacement utility poles, string new power lines, repair damaged substations, restore ground-level services, and conduct all the other missions necessary after traditional hazards. Utility workers are trained and equipped to perform these tasks safely and effectively, even in the midst of the effects of a storm as severe as Sandy. When Consolidated Edison and other utilities struck by Sandy determined that their own restoration capabilities were inadequate after the storm, the support missions they requested through the Regional Mutual Assistance Group system were precisely those that other utilities were already staffed and equipped to perform. And viewed from a nationwide perspective, these familiar restoration tasks are being performed every day of the year, including by the public power utilities and electric

cooperative utilities (which have their own mutual assistance systems).[39]

Moreover, the equipment that mutual assistance crews needed to repair after Sandy was largely similar to the equipment that they repaired for their home utilities. Variation does occur across circuit breakers, substation components, and other grid assets, but many other assets are generally similar across utilities, enabling Sandy mutual assistance personnel to quickly and easily contribute to line restringing and other restoration tasks.

This commonality stands in stark contrast to the proprietary utility-specific OT applications, device configurations, and ICS networks that would need to be restored after a cyber attack. Every utility in the United States has its own ICS architecture, often with nonstandard protocols, legacy systems that may be many years old, and irregular or extinct proprietary technologies.[40] Attempts to reconfigure ICSs by personnel who lack detailed knowledge of those systems can easily "brick" the systems and greatly complicate restoration efforts.

While the heterogeneity of today's control systems would hamper recovery efforts, it also has benefits for wide-area grid security. The enormous diversity of ICS software and control system components among utilities greatly complicates the task of conducting a "single-stroke" attack to black out an entire interconnect or the US grid as a whole, although it would not preclude an adversary from conducting the more targeted, limited-scale attacks examined in this study.

It is possible that the ICS supplier landscape will experience further consolidation over the next few years. If so, shared reliance on a shrinking set of component suppliers may create more similarities across utility systems, facilitating cross-training and mutual support between companies that rely on the same brands of operating systems (although utility-specific network design features would likely persist, with utility-specific configurations and data). However, some of these desirable features could also be achieved through robust standards for interoperability and data storage. This would effectively reconcile the recovery advantages afforded by homogeneity with the security advantages arising from heterogeneity. Further study is needed to assess strategies for encouraging the availability and use of a diverse yet robust set of critical infrastructure components.

Still, for now, the basic challenge remains: highly trained personnel who know how to repair their own utilities after a cyber attack will have limited ability to repair others. As an initial step to facilitate cross utility support, utilities could voluntarily develop and adopt detailed competency requirements and skill standards for OT specialists in their sector. A foundation for establishing competency requirements has been under way, with industry-specific guidance provided by the DOE including the *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)* and skills-focused research into the need for secure power system professionals. Utilities could build on this foundation by developing a typology for the skills required to assist power restoration after a cyber attack, creating shared terminology on restoration tasks and operations.[41] Then, within the mutual assistance systems managed by investor-owned utilities, public power companies, and electric cooperatives, utilities could begin the process of setting the competency requirements for post-cyber attack restoration assistance.[42]

[39] Miles Keogh and Sharon Thomas, *Regional Mutual Assistance Groups: A Primer* (Washington, DC: National Association of Regulatory Utility Commissioners, November 2015), http://www.slideshare.net/SharonThomas27/naruc-rmag-paper-1122015.

[40] NERC, *Cyber Attack Task Force*, 28.

[41] L. R. O'Neil et al., *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report* (Richland, WA: Pacific Northwest National Laboratory, July 2013), http://energy.gov/sites/prod/files/2013/12/f6/SPSP_Phase2_Summary_Final_Report.pdf.

[42] Another option for the Bulk Electric System (BES) would be inclusion of competency standards in the mandatory

The electricity sector could also explore opportunities to meet the challenges of cross utility training and support by starting with small-scale pilot mutual assistance initiatives. The nationwide mutual assistance system that exists today was not built in one step. It emerged over many decades, starting with agreements among a small number of utilities in individual states and regions and then gradually scaling up over time. Mutual assistance for cyber events might start in a similar fashion, with neighboring utilities establishing cross-training programs and joint exercises for mutual assistance and then gradually scaling up such collaboration into larger assistance agreements. In the cyber realm, however, geographic proximity could be less significant than the cross utility commonality of OT software and other network features. Mutual assistance initiatives might begin between utilities that share such network commonalities. Appropriately secure information-sharing mechanisms between utilities could help them identify potential partners for pilot programs far beyond their own states.

To develop such training and exercise programs, one practical approach could be to adopt a "crawl, walk, run" strategy to build mutual assistance capabilities in a sequenced fashion. Opportunities for support lie along a spectrum of difficulty in terms of the network-specific knowledge required for system restoration. Starting at the less difficult end of the spectrum and proceeding toward the more demanding, one utility might assist another by (1) assisting with the recovery of corporate IT systems; (2) scrutinizing network logs to identify anomalies and possible malware signatures; (3) supporting perimeter defenses against ongoing attacks; and (4) directly assisting OT component and system restoration. Assistance even on these less demanding tasks could be helpful because it frees up a utility's own cyber experts to concentrate on the more difficult tasks. Adopting a crawl, walk, run approach could also facilitate the gradual development of trust and cross network familiarity vital for providing assistance at the more difficult end of the spectrum.

The Electricity Subsector Coordinating Council (ESCC) and other coordinating bodies can help provide a broader framework for establishing and scaling up such assistance initiatives. The ESCC already is developing playbooks for incident planning and government–industry coordination.[43] As the playbook effort moves forward, the ESCC should help sponsor and oversee measures to overcome the technical challenges of utility-to-utility support, as well as help build the policies and coordination mechanisms that cyber mutual assistance will require.

Growing the Talent Pool

In the hurricane belt and other areas where severe storms frequently occur, or where earthquakes or other catastrophic events present significant risk factors, utilities build and maintain substantial capabilities for power restoration. Journeymen linemen and other contractor-provided assets supplement utility crews as needed. In terms of total potential capacity, these industry capabilities provide a vast pool of assets that can be drawn on by utilities in need, as exemplified by the massive deployment of repair personnel after Sandy.

The superstorm has also prompted industry to reassess the total amount of mutual assistance resources that might be required in future catastrophes. As noted above, investor-owned utilities are now structuring their mutual assistance system to prepare for national response events (NREs) that impact a large population

requirements for certified grid operators. The NERC Cyber Security Standards require awareness and training, but they fall short of establishing competency requirements and objectives for cyber defense roles instrumental in ensuring the security of reliability-critical OT and power restoration. However, voluntary adoption of such standards will likely provide a more immediate opportunity for progress.

[43] Critical Infrastructure Partnership Advisory Council, "Electricity Subsector Coordinating Council and Government Executives Meeting Agenda," June 15, 2015, https://www.dhs.gov/sites/default/files/publications/cipac-elec-scc-govt-exec-agenda-06-15-15-508.pdf.

or several regions across the United States and require resources from multiple regions to support power restoration. The NRE initiative has greatly improved the ability of industry to coordinate and allocate utility crews and other industry emergency restoration resources at the national level, including private contractors employed by utilities. The NRE initiative also explicitly recognizes that national events requiring such massive flows of mutual assistance could include acts of war.[44]

Public power utilities are also ramping up their mutual assistance agreements and capacity for providing aid. A number of these agreements are coordinated by state associations; in other cases, public utilities make arrangements directly with each other. Public utilities have also worked with the Federal Emergency Management Agency (FEMA), the National Rural Electric Cooperative Association (NRECA), and the American Public Power Association (APPA) to create an APPA/NRECA Mutual Aid Agreement, providing a much more comprehensive system for restoration assistance in region-wide or multiregional outages.[45] The APPA has also recently developed a national mutual aid network to support municipal utilities during disasters.

A much smaller pool of trained personnel can scrub malware and conduct other highly technical operations after a cyber attack. While utility personnel had comprehensive knowledge of the tasks required to restore power after Sandy, restoring ICSs that the adversary has covertly reconfigured to misoperate is a much less familiar mission. The same is true of scrubbing APTs from firmware or the broad range of other tasks that may be required against the 2020–2025 threat.

A growing number of utilities rely on private companies to provide skilled personnel for restoration operations. When hurricanes and other natural hazards occur, utilities often rely on journeymen construction linemen and other contractor personnel to augment their own staffs because having these assets on call is less costly than maintaining additional full-time crews on the utility's payroll. A similar approach might be taken to supplement utility personnel trained for post-cyber attack restoration, as long as contractors were familiarized in advance with the specific OT networks, software applications, and restoration protocols on which individual utilities will rely.

However, the same risk of multiple nationwide cyber attacks that complicates mutual assistance agreements could also create problems when relying on contractors. Individual companies may be called on to serve multiple clients at the same time (in both the public and the private sectors), requiring staffing levels far beyond those necessary for the typical levels of support. Contractor surge capabilities will be essential to meet such demands; otherwise, utilities will be left without the assistance they need.[46]

As an alternative to relying on contractors, many utilities are increasing their own staff capabilities for post-cyber attack power restoration. No publicly available report specifies the number of utility personnel who are trained to repair and restore OT systems. However, based on an initial survey conducted for this study, elements of the sector appear to vary widely in the size of the trained staffs they maintain. One large regional transmission organization (RTO) retains more than two hundred personnel to meet its estimate of its own post-cyber attack restoration requirements. In contrast, a major

[44] Edison Electric Institute, *Mutual Assistance Enhancements* (Washington, DC: Edison Electric Institute, October 2013), 2, http://www.eei.org/issuesandpolicy/RES/TAB%205.pdf.

[45] William Atkinson, "Mutual Aid Comes of Age," *Public Power* 70, no. 2 (March–April 2012), http://www.publicpower.org/Media/magazine/ArticleDetail.cfm?ItemNumber=34001.

[46] One possible means for providing such a surge capacity, currently under development in the electricity sector, is the creation of critical power restoration teams that would draw on engineering-based industry partners in the aerospace sector and beyond. Electric Infrastructure Security Council, http://www.eiscouncil.com/.

utility that distributes electricity over multiple states has fewer than fifty staff members to assist both information technology and OT restoration. Smaller utilities have little or no such organic capability and would need to rely on mutual assistance or private sector OT service providers (who could face widespread demands for support in attacks that create multiple recurring outages).

The shortage of available OT specialists for electric utilities is part of a broader nationwide shortfall across government and other critical infrastructure sectors. The dean of the National Security Agency's College of Cyber notes that "the demand is huge" for such experts. "Industry needs them. The government needs them. Academia needs them. And right now there's just not enough. Everyone is stealing from each other."[47]

High-quality training programs for OT security, such as those conducted by the DHS ICS-CERT, can help utilities grow their cyber-capable workforces. But the capacity of these training programs is limited. They would have to be substantially expanded to grow the pool of personnel needed for post-cyber attack power restoration.[48] Expansion would also be needed in the throughput of utility personnel in ICS defense and incident response training programs conducted by the SANS Institute and other providers.[49]

Expanded exercise systems will also be essential to expand the cyber workforce and build cross utility expertise. GridEx, Cyber Guard, and other existing exercises are extremely valuable, but they are not conducted with sufficient frequency or scale to serve the learner community that utilities require. A sustained exercise system using realistic scenarios, distributed interactive play, and shared standards for assessment and certification will be essential to supplement the exercises currently in place.

Such growth would come at considerable expense and would merit rigorous cost–benefit analysis before being undertaken. Moreover, even if such an effort proved to be cost beneficial, considerable time would be required to grow an appropriately sized workforce. Until utilities and their partners can expand the pool of available talent, the scarcity of cyber-capable specialists will exacerbate the previously noted problems for mutual assistance systems. In a cyber attack, unlike in an event like Sandy, utilities may be reluctant to send assistance crews for mutual assistance because the adversary could strike anywhere in the United States. The vastly smaller pool of trained personnel for post-cyber attack restoration, versus those available for stringing line or erecting poles after a storm, will tend to make utility CEOs even more likely to keep those assets close to home where they might be needed at any moment.

Increasing the trained staffs for cyber response in the electricity sector capabilities would ease the problems of mutual assistance for cyber attacks but would not fully resolve them. Even substantially augmented staffs would likely be unable to assist other utilities unless they are cross-trained to do so and gain sufficient familiarity with these other OT systems to be of value. Utilities could explore such cross-training opportunities as part of a broader analysis of alternatives that will assess US power restoration requirements, the array of options to meet them, and criteria for evaluating those options.

[47] Darren Samuelsohn, "Inside the NSA's Hunt for Hackers," *Politico*, December 9, 2015, http://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330.

[48] Brent Stacey, associate director of the Idaho National Laboratory, detailed the rationale for such an expansion. See *United States House of Representatives Science Subcommittee on Energy and Science Subcommittee on Research and Technology* (October 21, 2015) (statement of Brent Stacey, Associate Director, Idaho National Laboratory), http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf.

[49] ICS515: ICS Active Defense and Incident Response, course offered by SANS Institute, https://www.sans.org/course/industrial-control-system-active-defense-and-incident-response.

Replacing Damaged Equipment

The storm surge and weather effects during Sandy inflicted extensive physical damage on electricity substations and other critical grid components. As in Sandy, utilities can reroute power around damaged equipment to help speed power restoration. Such rerouting opportunities may also exist in response to cyber attacks (although it will be essential to prevent the spread of malware from one utility to the next). To further accelerate restoration time lines, utilities have also established programs to supplement their own stores of replacement equipment by drawing on cross utility programs to share grid components. In particular, initiatives such the Spare Transformer Equipment Program (STEP), SpareConnect, and the Grid Assurance initiative help enable utilities to support each other by providing spare high-voltage transformers and other components.[50] Although these programs emerged to mitigate the risk of physical damage caused by natural hazards or kinetic attacks, they could also serve as a model for creating equivalent initiatives to accelerate the replacement of equipment that is bricked or otherwise destroyed by malware.

The 2012 cyber attack on the Saudi Aramco oil company exemplifies the potential benefits of building such equipment-sharing mechanisms. That attack reportedly required the replacement of thousands of office PCs whose hard drives had been wiped.[51] If US power companies identify grid equipment that is at similar risk of large-scale damage, they might supplement their own cyber-protected spares by establishing programs to share replacements, thereby accelerating power restoration.

However, the Saudi Aramco attack did not strike the company's OT systems. Spare equipment replacement initiatives for the US grid would need to account for the risk that adversaries will disable programmable logic controllers and other OT equipment. Uncertainties also persist over the degree to which adversaries will be able to inflict widespread damage on generators or other difficult-to-replace grid components. Additional research will be essential to clarify these risks before equipment replacement programs can be sized and structured to mitigate them. Moreover, given the inherent difficulties of repairing and replacing generators, measures to protect them from attack (as opposed to building programs to restore these assets after they are damaged) are likely to offer a better way to strengthen grid resilience.

Challenge 3: Concepts of Operation to Accelerate Industry Power Restoration

When hurricanes and other familiar hazards strike the electric grid, affected utilities and those providing mutual assistance have well-understood and frequently exercised plans and operating principles to guide restoration efforts. The electricity sector is developing equivalent principles for post-cyber attack restoration. A critical step in that process will be to develop a consensus-based CONOPS to accelerate the restoration of electric service and help deny adversaries the political and military effects they seek to achieve by attacking the grid.

To be most useful to the power sector, such a CONOPS should concisely describe the structure for an industry-wide restoration system for cyber threats (as opposed to natural hazards). The CONOPS should also identify guiding principles for how the electric industry will use that system, and how utility partners in the public and private sectors should support restoration operations.[52]

[50] "Spare Transformers," Edison Electric Institute, http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

[51] Jim Finkle, "Exclusive: Insiders Suspected in Saudi Cyber Attack," *Reuters*, September 7, 2012, http://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907.

[52] For guidelines on developing CONOPS, see IEEE Computer Society, *IEEE Guide for Information Technology—System*

The analysis that follows identifies key issues and recommendations for the development of such a CONOPS by the two basic components of the US electric system: (1) electric distribution utilities and (2) Bulk Electric System (BES) entities, which include the owners and operators of electrical generation resources, high-voltage transmission lines, interconnections with neighboring systems, and associated equipment.[53] Although regulated differently, both components will confront shared challenges in post-cyber attack power restoration and will need to be integrated into holistic sector-wide resilience efforts.

Key Components of a Cyber Restoration Concept of Operations for Distribution Utilities

For blackouts caused by hurricanes or other natural hazards, the utilities struck by the event play a central role in assessing damage to their infrastructures and developing plans to guide and prioritize restoration efforts. Utilities typically have well-developed and frequently exercised emergency management procedures to conduct such operations. They are also incorporating advances in distribution automation, smart meters, and other smart grid technologies to remotely pinpoint outage locations and accelerate power restoration. Utilities use these systems to help generate work tickets to replace downed poles and repair other damaged infrastructure and to oversee restoration efforts by their own crews and those provided by other utilities under mutual assistance agreements, all in alignment with familiar emergency procedures for re-energizing the grid.

Different procedures and organizing principles will be required when responding to cyber threats. The first challenge that distribution utilities will face is detecting that an attack is under way and determining how adversaries are disrupting utility systems. During Sandy and other natural hazards, knowing that a destructive event is occurring is simple. Determining which poles are downed and need to be replaced is equally straightforward. Cyber attacks on ICSs pose different and much more difficult detection and damage assessment challenges, especially against APTs designed to hide on utility networks. Adversary-imposed changes in control system networks and operating instructions can be difficult to discover. Attack detection is further complicated because few ICSs maintain logs of changes to them, and legacy technology in OT networks (including outdated software and third-party applications) may provide multiple opportunities for adversary exploitation. The first indication that an attack is under way may be when HMIs begin to "gray out," equipment begins to misoperate, and power systems begin to fail. Opportunistic adversaries might even time their strikes to coincide with a hurricane, earthquake, or other severe natural event, thereby further complicating efforts to determine that a cyber attack is under way.

Power restoration against cyber attacks will require the ability to rapidly detect the malware or other attack mechanisms that are disrupting utility operations. Once detected, that malware must be analyzed so that countermeasures can be developed against it. Those countermeasures can then be deployed as utilities search for and eradicate that malware throughout their ICSs and reestablish the integrity of their networks.

Organizing Principles

Few if any utilities will have sufficient in-house technical expertise to reverse-engineer malware and develop effective network inspection and mitigation measures against APTs. Private contractors can assist

Definition—Concept of Operations (ConOps) Document, IEEE Standard 1362-1998 (Piscataway, NJ: IEEE, March 19, 1998).

[53] NERC, *Glossary of Terms Used in NERC Reliability Standards* (Washington, DC: North American Electric Reliability Corporation, September 29, 2015), 14–16, http://www.nerc.com/files/glossary_of_terms.pdf. Note that although distribution utilities and BES components are regulated differently, many of the largest US utilities own and physically operate both high-voltage transmission (BES) and distribution systems, creating significant overlap between these sector components.

utilities in such efforts. However, to provide more robust and broadly available sources of technical assistance, including from government sources, a highly coordinated system would be needed to rapidly analyze utility logs and data, catalog and analyze malware provided by utilities, and develop remediation measures. Such a support system would also need the ability to quickly deliver those measures back to utilities struck by the attack (and also warn and deliver prevention measures to block attacks on other utilities).

However, as already noted, individual utilities have the best understanding of their own network structures, applications, and other features and will have unmatched experience and expertise in managing their network operations. Their personnel—and those from utilities cross-trained to work on their networks—will need to play a crucial role in applying the remediation measures developed by supporting organizations. Accordingly, the power restoration system should be organized on the principle of tightly coordinated support and distributed utility-led execution. Subsequent portions of this paper examine how industry and government can partner to help provide utilities with such tightly coordinated support on malware signature identification, remediation measures, and other forms of technical assistance.

Principles for Emergency Operations and Power Restoration

CONOPS for post-cyber attack restoration will also require cyber-specific guiding principles and shared best practices for power restoration. APTs differ from natural hazards in that they can be designed to reattack utility networks if not completely eradicated and can also spread across utility components (and, potentially, from one utility to many others). Both of these threat characteristics will create challenges for restoration beyond those already discussed for mutual assistance.

Moreover, adversaries are intelligent and adaptive in ways that natural hazards are not. As adversaries modify their means of attacking in response to electricity sector and US government countermeasures, a centralized support/decentralized implementation system will not only need to be able to sustain operations during reattacks, but it will also need to keep pace with adversaries' adaptations.

Unlike hurricanes, cyber attacks can also seek to corrupt system integrity and manipulate data and control sensors on which utilities rely to provide reliable and resilient service. Major utilities typically use energy management systems (EMSs) that provide highly redundant hardware, software, and telecommunications components to help sustain their operations and support restoration as needed. These systems and the data they carry will be prime targets for attack. Malware that can propagate across networks, and use utility assets to disrupt other grid components linked to them, will pose additional problems for defending these systems and restoring them if an attack occurs.[54]

To meet the novel challenges posed by cyber threats, a number of utilities are developing a tiered approach to sustaining service during an attack and restoring service once disruptions occur. These measures include (1) hardening their primary control centers against attack; (2) building robust backup control centers; (3) securing their gold copies of OT system software and exercising to rapidly install it if needed; (4) developing "spare-tire" control mechanisms that will not provide the full functionality of regular systems but can sustain limited vital operations; and (5) maintaining fallback mechanical controls that would otherwise be at risk of degrading and becoming inoperable. Many of these same initiatives are also being adopted or developed by high-voltage transmission companies, RTOs, and other BES entities.

[54] NERC, *Severe Impact Resilience*, 35.

Utilities may want to accelerate and expand their sharing of potential best practices and restoration guidelines. The CONOPS for restoration should provide guidelines and operating principles on the following:

- How to operate a system that has lost its integrity and experienced a cyber incident that has demonstrated the ability to disrupt, misoperate, or physically damage equipment
- The communication and operating protocol that impacted utilities follow
- What neighboring and interconnected utilities should do with their data connections to the impacted utility
- How utility systems' components might be safely taken off-line to limit the spread and reduce the consequences of an attack (especially physical damage to grid equipment), thereby accelerating restoration

Developing an Integrated Restoration Strategy for the Bulk Electric System and Distribution Utilities

To disrupt distribution utilities' ability to sustain service to defense installations and other critical US assets during a crisis, cyber adversaries may attack those utilities directly, but they may also strike the BES that provides power to distribution systems. Adversaries can also attack the BES to cause wider-area outages. If cyber attacks can damage or disrupt the generation plants, high-voltage transmission systems, and interconnections with neighboring systems that make up the BES, adversaries may be able to affect multiple distribution systems and potentially cause cascading grid failures across broad regions of the United States. A CONOPS to accelerate post-cyber attack power restoration will need to encompass both BES and distribution utilities in an integrated way. Digital assets at nuclear power plants are subject to standards set by the Nuclear Regulatory Commission; these plants, too, should be part of a holistic approach to cyber resilience.

NERC standards require that utilities with BES assets maintain both primary and backup EMSs and meet a growing set of critical infrastructure protection (CIP) reliability standards in response to cyber threats.[55] RTOs and other components of the BES also have long-established principles to sustain service and guide restoration operations after natural hazards. When faced with an approaching storm such as Sandy, RTOs can go into conservative operations to help maintain the reliability of the BES. They can purchase additional power reserves, making more resources available to respond to unexpected events, staff up their backup control centers, and take additional measures before a storm hits. When damage to the grid begins to occur, they can route power around disabled substations and other complements and reconfigure their systems to limit the areas that lose electric service and help accelerate the restoration of power.[56]

[55] NERC, *Cyber Security Reliability Standards CIP V5 Transition Guidance: ERO Compliance and Enforcement Activities during the Transition to the CIP Version 5 Reliability Standards* (Washington, DC: North American Electric Reliability Corporation, August 12, 2014), http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf. For broader principles and plan elements to guide BES guide restoration operations, see "Electric System Restoration Reference Document," in NERC, *NERC Operating Manual* (Washington, DC: North American Electric Reliability Corporation, August 2014), ESR-5–ESR-6, http://www.nerc.com/comm/OC/Pages/Operating-Manual.aspx.

[56] For examples of conservative operation triggers and response actions, see PJM, *Fundamentals of Transmission Operations: Conservative Operations* (Audubon, PA: PJM, October 3, 2013), http://www.pjm.com/~/media/training/new-pjm-cert-exams/foto-lesson9-conservative-operations.ashx; MISO, *MISO Operating Procedures* (Carmel, IN: MISO, 2015), https://www.misoenergy.org/Library/Repository/Communication%20Material/One-Pagers/One%20Pager%20-%20MISO%20Operating%20Procedures.pdf; and SERC Reliability Corporation, *Guideline: Conservative Operations Guidelines* (Charlotte, NC: SERC Reliability Corporation, May 20, 2015), http://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.

Equivalent mitigation measures and principles to support power restoration may be essential when responding to cyber attacks. Some measures, such as standing up backup control centers, will be similar to those required for traditional hazards. Others may be cyber specific: for example, efforts to protect or reestablish the integrity of telemetry data on which RTOs rely. NERC's report on severe impact resilience (2012) proposes an array of options to help protect BES components from possible physical damage, preserve the integrity of BES data and systems, and limit the spread of malware across the US grid. Possible measures include the following:

- Disable supervisory control and data acquisition (SCADA) and communications networks from substations and generation facilities
- Disconnect relays from breakers
- Segment the power grid into preplanned islands (and effectively manage the unplanned islands the cyber attack creates)
- Isolate network connections to the Internet
- Safely shut down systems to deny an attacker the ability to cause further damage[57]

Although measures could be useful to blunt cyber attacks and downsize the power restoration requirements that BES entities would face, many of them could also seriously disrupt the ability of RTOs and other entities to sustain service or monitor and control grid operations. Realistic exercises will be vital to determine whether and how these options might best be used and how the consequences (and potential liability issues) associated with intentional service interruptions can be mitigated.

Energy Management Systems for Cyber Events

As noted above, NERC requires utilities with BES assets to maintain both primary and backup EMSs to manage those assets, including generators, high-voltage transmission lines, and interconnections with neighboring systems. EMSs include highly redundant hardware, software, and telecommunication components to maximize the availability and accuracy of data utilities needed to manage the grid. This redundancy makes EMSs extremely reliable after hurricanes and other familiar hazards. With cyber attacks, however, EMSs will be at special risk. To the extent that the redundant EMS components are of the same make and model as those used in the primary system, they may also fail during a cyber attack unless they are protected against infection or reinfection by persistent malware. Moreover, precisely because EMSs will be so vital for limiting the impact of cyber attacks on the grid and for accelerating power restoration, they may themselves be targeted for disruption.[58]

To mitigate the risk that adversaries will disable or corrupt both primary and backup EMSs and data, a growing number of utilities are developing independent, secured fallback systems to use in emergencies. These spare-tire management systems provide only those capabilities that are minimally necessary to operate key BES components. While grid operators performing the roles of balancing authority and reliability coordinator are trained to manually calculate critical data required to operate their portions of the BES, spare-tire systems can provide valuable support for such operations. In particular, such spare-tire systems can help utility personnel operate crucial assets to maintain load and generation balance by monitoring and controlling a core of generation units and tie lines for

[57] NERC, *Cyber Attack Task Force*, 63; and NERC, *Severe Impact Resilience*, 18–50. Note that many of the recommendations in the resilience study apply to noncyber hazards, including coordinated kinetic attack.

[58] For an analysis of potential EMS vulnerabilities and mitigation options, see NERC, *Industry Advisory: Preventable SCADA/EMS Events – II* (Washington, DC: North American Electric Reliability Corporation), http://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/Preventable_SCADA_EMS_Events_II.pdf.

a specific geographic area. A basic level of automatic generation control functionality from such a system can also help operators to maintain stability within their systems and the interconnections with their neighboring utilities.[59]

As with any EMS, these spare-tire systems require a mathematical model that represents the electrical and operational characteristics of the BES assets being monitored and/or controlled, a database for rendering operator displays, and reliable telecommunications connectivity between the core BES assets. Preplanning for the operation of these systems will also be vital to account for the varying designs and configurations of assets that make up the BES and the diverse telecommunications components that utilities use. DOE national laboratories or other research facilities could support such integrative efforts by developing additional software tools to support grid-wide emergency operations and by providing a common training platform for the use of spare-tire systems.

Managing Conflicts between Mission Priorities

The CONOPS will also need to help utilities and their government partners resolve potential conflicts between efforts to attribute the cyber attack to a specific adversary and operations to restore power. To retaliate against an attack (and to be able to credibly deter attacks), the United States must have the ability to determine the source of the attack, even when an adversary uses remote botnets or takes other measures to complicate attribution.

Acquiring and preserving forensic data from the attack will often be essential for attribution. Ideally, system operators will be able to capture live system data (i.e., current network connections and open processes) before a machine suspected of being compromised is disconnected from the network. But exercising such restraint in a large-scale attack will be difficult and perhaps inappropriate.

Indeed, many of the recommended best practices to support forensics and attribution may directly conflict with the imperative to restore grid functionality as rapidly and effectively as possible. Utilities are cautioned against running antivirus software after an attack because an antivirus scan changes critical file dates, which impedes discovery and analysis of suspected malicious files and time lines. ICS-CERT also warns system operators against making any changes to the operating system or hardware, including updates and patches, because they will overwrite important information about the suspected malware.[60] Quickly reconciling these potential conflicts between forensics and power restoration will be essential to build US preparedness for post-cyber attack operations.

In December 2015, the Defense Advanced Research Projects Agency launched the Rapid Attack Detection, Isolation and Characterization (RADICS) initiative to advance the development of forensic tools that will require less delay or disruption of system restoration operations.[61] In the end, however, it may not be technically or operationally possible to fully deconflict these missions. Delayed restoration may be the price of effective attribution.

Funding Improved Utility Capabilities for Power Restoration and Mutual Assistance

Utilities' initiatives to increase cyber-qualified staffs and make other investments in cyber resilience will

[59] Data provided by a major electric utility that asked to remain anonymous.

[60] *ICS-CERT Monitor*, July/August 2011 issue, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf.

[61] Defense Advanced Research Projects Agency, *Broad Agency Announcement: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)*, DARPA-BAA-16-14 (Arlington, VA: Defense Advanced Research Projects Agency, December 11, 2015), 10–13, https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-16-14/listing.html. See especially Technical Area 3.

cost money. At a time when many utilities face flat revenues and confront other business challenges, clarifying how they will be able to recover their costs for such investments is a critical issue. These cost recovery issues may be even more challenging for power generation companies that rely on market revenues and do not have cost-of-service rates.

NERC's CIP reliability standards provide BES entities not only with requirements to meet but also with an objective basis for determining whether proposed investments in cyber resilience are necessary to meet those requirements and should therefore be eligible for cost recovery. BES entities can also request that their regulated transmission tariffs include the cost of resilience investments above those required for compliance with minimum standards.[62]

In contrast, state PUCs are responsible for ruling on proposed resilience investments made by the investor-owned utilities that distribute the vast majority of electricity in the United States. PUCs have a long record of allowing utilities to recover their costs for maintaining system reliability after typical storms and other natural hazards, including staffing and equipment for restoration operations. Sandy created a wave of new rate cases and tariff proposals by utilities to build their resilience against less frequent but especially destructive events. PUCs have deemed many, but far from all, of these investment proposals to meet their requirement that they be "prudent" and cost-effective.

Cyber attacks present a more difficult challenge for cost recovery. For flooding, hurricanes, and other natural hazards to the power grid, ample historical data exist to help predict the likelihood of an event (although rising sea levels and the increasing severity of storms is driving updates in many of these predictive models). Data on the likelihood of an event occurring at a given level of severity provide a basis to assess the potential benefits of investments against such events and whether those investments are prudent and worth their costs.

No historical data are available to predict the likelihood of a destructive cyber attack or other man-made threats to the power grid. Potential adversaries are continually probing and mapping the electricity sector in ways that can facilitate future attacks. However, the probability of a future attack occurring on a specific utility is not only unknown, but it is unknowable. Assessing the prudence of investments against such hazards is far more difficult. Indeed, PUCs are only beginning to build decision-making criteria that can allow them to assess the prudence and cost effectiveness of proposed investments in post-cyber attack restoration capabilities. Until clear, objective criteria exist, electricity distribution companies that want to strengthen these capabilities are at risk of having PUCs deny the funding needed to recover their costs.

The National Association of Regulatory Utility Commissioners has recognized the growing significance of cyber threats to the electric industry and has recommended a useful list of discussion points for engaging with utilities on cyber preparedness issues.[63] PUCs in states such as Connecticut and Pennsylvania are also developing strategies and recommendations to strengthen grid resilience against these threats.[64] However, these

[62] US Federal Energy Regulatory Commission, *Extraordinary Expenditures Necessary to Safeguard*, Docket No. PL01-6-00096 FERC ¶ 61,299 (2001) (statement of policy), http://www.iso-ne.com/committees/comm_wkgrps/trans_comm/tariff_comm/mtrls/2002/oct102002/A4_1466800.pdf.

[63] Miles Keogh and Christina Cody, *Cybersecurity for State Regulators, with Sample Questions for Regulators to Ask Utilities* (Washington, DC: National Association of Regulatory Utility Commissioners, February 2013), http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf.

[64] Pennsylvania Public Utility Commission, *Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities* (Harrisburg, PA: Pennsylvania Public Utility Commission), http://www.puc.pa.gov/general/pdf/Cybersecurity_Best_Practices_Booklet.pdf; and Connecticut Public Utilities Regulatory Authority, *Cybersecurity and Connecticut's Public Utilities* (New Britain, CT: Connecticut Public Utilities Regulatory Authority,

strategies primarily focus on prevention and offer little or no guidance on measures to accelerate power restoration. They are only beginning to define criteria for cost recovery. The Connecticut strategy calls for technical meetings between regulators and utilities to establish performance standards for managing cyber threats.[65] Such discussions should occur between PUCs and utilities nationwide to help build consensus on prudence and cost-effectiveness criteria for investments in cyber resilience, including capabilities to accelerate power restoration.

Additional funding for utility investments might come from DOD and other federal departments responsible for US security. Given the risk that adversaries will target the grid to disrupt the execution of critical missions at defense installations, and the importance of accelerated power restoration to those installations, a strong rationale exists for military bases to partner with their neighboring utilities to improve grid resilience against cyber threats.[66] Exploratory partnership initiatives are already under way, most notably the DOE-supported Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) microgrid demonstration project conducted with the Hawaiian Electric Company for Camp Smith, Hawaii. The project seeks to demonstrate how utilities and DOD can partner to develop a secure microgrid architecture for military installations, including distributed and renewable power generation and energy storage. The project has also examined whether and how such developments might be used by nonmilitary facilities and critical infrastructure.[67]

Intense competition for funding within DOD will limit the department's ability to scale up these projects on a nationwide basis. Instead, the DOD could develop new business models for public–private partnerships with utilities, including ways to price resilient electric service so that utilities can recover the costs of providing for rapid power restoration and other prudent investments in cyber resilience. DOD's *Energy Resilience Business Case Analysis Study* (commissioned April 2015) provides an important initial step in this direction.[68] That study, and associated efforts to strengthen energy resilience for the military bases, could become the focus of expanded discussions between DOD and the electric industry.

Government Support for Utility Restoration Operations

Campaigns such as BlackEnergy have already demonstrated the value of existing mechanisms of government support to the electricity sector. The ability of DHS's ICS-CERT to meet industry requests for assistance (RFAs) and help utilities identify and counter malware implanted on their systems provides a model of effective federal support.[69] A growing number of state National Guard organizations and other state agencies are also pursuing initiatives to help grid owners and operators deal with ongoing cyber intrusions.

However, an attack with a national security impact like that of the targeted threat scenario described in this study would create an entirely different operating environment. Such an attack could also spur industry requests for government cyber assistance far beyond those that state and federal agencies are currently

April 14, 2014), http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.

[65] Connecticut Public Utilities Regulatory Authority, *Cybersecurity and Connecticut's Public Utilities*, 25.

[66] On the broader national security rationale for DOD–utility partnerships, see Department of Defense, *Mission Assurance Strategy*, April 2012.

[67] "SPIDERS JCTD Smart Cyber-Secure Microgrids," US Department of Energy, http://energy.gov/eere/femp/spiders-jctd-smart-cyber-secure-microgrids.

[68] US Department of Defense, Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, *Energy Resilience Business Case Analysis Study* (Washington, DC: US Department of Defense, forthcoming).

[69] "Alert (ICS-ALERT-14-281-01B)."

prepared to meet—that is, if industry can first identify what kinds of support would actually be useful.

The Post-Sandy System for Government Support to Utilities

Sandy has driven major improvements in federal and state agency preparedness to support power restoration. This emerging support system can help provide a foundation for assistance after cyber attacks on the grid. Indeed, because key components of this system are still evolving, now is the ideal time to clarify how the system should be adapted and supplemented to help utilities meet emerging cyber threats.

DOE is playing a key role in shaping the post-Sandy system for government support in power restoration operations. DOE is the federal coordinator and primary agency for Emergency Support Function (ESF) #12, Energy. ESF #12 states that "restoration of normal operations at energy facilities is the responsibility of the facility owners." However, when industry requests federal support for power restoration, ESF #12 is "the primary Federal point of contact with the energy industry" for such requests. More broadly, under DOE leadership, ESF #12 is "intended to facilitate the restoration of damaged energy systems and components" for events requiring a coordinated federal response.[70] DOE is also the energy sector-specific agency, which gives it additional leadership responsibilities in responding to non-Stafford Act emergencies.

DOE's Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement (February 2013) identified a number of areas in which the department's plans and organizational arrangements "fell far short of what was needed to respond, mitigate, and restore the damaged energy infrastructure."[71] Two shortfalls proved especially critical and are now the focus of DOE initiatives to strengthen the department's support for future restoration operations.

First, Sandy revealed that DOE lacked the organizational structure needed to provide adequate situational awareness of power outage locations and restoration time lines. DOE's structure also failed to specify where and how utility representatives would tie in to the department and provide industry priorities for support. Under the OE-30 Energy Response Organization structure, DOE is now reorganizing itself to overcome these shortfalls and help strengthen its ability to support emergency response operations.[72]

Second, during Sandy, DOE lacked adequate plans to guide its response operations. In partnership with FEMA, the department was very successful in improvising during the superstorm, developing the mechanisms and decision-making systems to coordinate government responses to industry RFAs. But it would have been far better to have had a plan already in place. DOE's *Energy Response Plan*, version 1.0, takes initial key steps to establish such a plan.[73]

Sandy is also spurring FEMA's progress on power restoration support. As with DOE, FEMA is exploring new structural arrangements to support power restoration and build on lessons learned from the

[70] US Department of Energy, *Emergency Support Function #12–Energy Annex* (Washington, DC: US Department of Energy, January 2008), 1–2, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nrf-esf-12.pdf.

[71] US Department of Energy, *Overview*, 7.

[72] US Department of Energy, *OE-30 Energy Response Organization* (Washington, DC: US Department of Energy, August 2015). To help meet the special challenges of establishing situational awareness during a cyber attack, including assessing the risk that adversaries will spoof or corrupt telemetry data, the Defense Advanced Research Projects Agency RADICS initiative includes an effort to develop regional situational awareness technologies with reduced vulnerabilities to such risks. Defense Advanced Research Projects Agency, *Broad Agency Announcement: RADICS*, 7–8.

[73] US Department of Energy, *The DOE Energy Response Plan*, version 1.0 (Washington, DC: US Department of Energy, February 2015), 6–7.

creation of the Energy Restoration Task Force during Sandy.[74] FEMA and DOE are also collaborating to develop a new framework, the Power Outage Incident Annex (POIA), to coordinate federal assistance in outages even more severe than after Sandy. The POIA will describe the process and organizational constructs that the federal government will use to respond to and recover from loss of power resulting from natural or unnatural disasters. Among other tasks, the POIA is designed to identify key federal government capabilities and resources, prioritize core capabilities, and outline response and recovery resource requirements.[75]

Cyber threats should figure prominently in the man-made hazards that the POIA addresses. More broadly, to the maximum extent possible, the emerging post-Sandy system for federal restoration support should provide the foundation for assistance in cyber attacks. As with industry's mutual assistance system, adopting such an all-hazards approach will avoid the operational risks and inefficiencies associated with building stovepiped mechanisms for government assistance. Yet, as in industry, an all-hazards approach will also have to account for the types of assistance that utilities are likely to need and the unique operating environment that a cyber attack on the United States would create.

Information and Intelligence Sharing

Before Sandy hit, the National Oceanic and Atmospheric Administration (NOAA) provided critical warning of the storm's likely path. By providing timely and accurate forecasts to emergency managers and the private sector, NOAA helped utilities and their government partners mobilize and stage resources to accelerate power restoration. NOAA is strengthening its modeling capabilities to provide still greater predictive accuracy in the future.[76]

Information requirements for cyber attacks will be entirely different but equally vital. As with Sandy's storm track, the occurrence of an intense regional crisis may provide advanced warning that a cyber attack could occur, as opposed to a "cyber Pearl Harbor" strike launched as a total surprise. The ability of the federal government to share classified information on the emerging risks of an attack could provide valuable time for utilities to stand up their emergency management systems, accelerate their network protection measures, and prepare for mutual assistance operations.

Once an attack is under way, utilities across the United States will need the fastest and most accurate data possible on threat signatures and remediation measures. The E-ISAC, in collaboration with DOE and the ESCC, serves as the "primary communications channel for the Electricity Sector" and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.[77] In particular, the E-ISAC helps the sector establish "situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange."[78] The ESCC, in turn, serves as the principal liaison between the federal government and the electric

[74] FEMA, *Hurricane Sandy FEMA After-Action Report*.

[75] US Government Accountability Office, *Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Address Electromagnetic Threats to the Electric Grid*, Statement of Christopher P. Currie, Director, Homeland Security and Justice, Before the Committee on Homeland Security and Governmental Affairs, US Senate (Washington, DC: US Government Accountability Office, July 22, 2015), 8, http://www.gao.gov/assets/680/671971.pdf.

[76] Louis Uccellini, "Sandy—One Year Later," *Weather Ready Nation*, October 28, 2013, http://www.nws.noaa.gov/com/weatherreadynation/news/131028_sandy.html#.VqvIaLEo7Gg.

[77] Patricia Hoffman, Assistant Secretary of Energy, Letter to Gerry Cauley, March 14, 2013, http://www.nerc.com/news/Headlines%20DL/ES-ISAC%20Letter%2014MAR13.pdf; and "Electricity ISAC," North American Electric Reliability Corporation, http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

[78] "Electricity ISAC," North American Electric Reliability Corporation.

power sector on issues pertaining to "joint planning, preparedness, resilience, and recovery related to events of national significance that may affect the secure and resilient supply and delivery of electricity," including cyber attacks.[79]

DHS can also provide information to support restoration operations. The ICS-CERT provides an especially important resource. Managed and operated by the DHS Control Systems Security Program and operated in coordination with the US Computer Emergency Readiness Team, ICS-CERT provides focused operational capabilities for defense of control system environments against emerging cyber threats. Specific support missions include the following:

- Responding to and analyzing control systems-related incidents
- Analyzing vulnerabilities and malware
- Developing situational awareness in the form of actionable intelligence
- Coordinating the responsible disclosure of vulnerabilities/mitigations
- Sharing and coordinating vulnerability information and threat analysis through informational products and alerts

At the state and local levels, fusion centers can provide utilities with an additional source of threat information to facilitate protection and power restoration operations. As in the case of the Kansas Intelligence Fusion Center, the presence of the National Guard at these centers can provide for especially valuable reachback to federal sources of classified threat data to share with cleared industry personnel. The Federal Bureau of Investigation and DHS can also provide valuable data to utilities through fusion centers and other sharing mechanisms.

However, fusion centers vary widely in their capacity to support post-cyber attack power restoration. Not all of them have provided for adequate representation by utility personnel during such emergency operations. They also vary in the degree to which they are building on the successful model of the Kansas Intelligence Fusion Center and capitalizing on opportunities for National Guard reachback for classified information. DHS and the Information Sharing and Access Interagency Policy Committee should encourage fusion centers to treat support for power restoration as a priority within their broader responsibilities to strengthen cyber resilience.[80] DHS could also adjust the grant guidance it provides to fusion centers to recognize and support the vital role that centers can play in strengthening the cyber resilience of the grid and other critical infrastructure sectors.

However, unless the flow of data from these disparate organizations can be integrated and provided in an efficient way, utilities could face an unmanageable number of "touchpoints" to get the assistance they need. A tightly coordinated approach will also be vital to facilitate the flow of information in the reverse direction: that is, from utilities to support organizations, so that utilities can provide samples of malware and other aspects of the cyber attack that they discover on their networks.

Progress is under way in providing for such coordinated information flows. In particular, the Cybersecurity Risk Information Sharing Program is already helping twenty operating companies (representing 65 percent of US customers) and their government partners accelerate the sharing of unclassified and classified threat information from multiple sources and develop situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection

[79] US Department of Homeland Security, *Electricity Sub-Sector Coordinating Council Charter* (Washington, DC: US Department of Homeland Security, August 5, 2013), https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf.

[80] US Department of Homeland Security, *Coordinating Federal Support for Fusion Centers* (Washington, DC: US Department of Homeland Security, August 2012), http://www.dhs.gov/sites/default/files/publications/coordinating-federal-support-for-fusion-centers-flyer-compliant.pdf.

of their critical infrastructure.[81] Utilities should play a leading role in determining how these and other information-sharing mechanisms should be coordinated and centralized to most efficiently support them. Of course, a more centralized two-way information-sharing system would also create an especially high-value target for attack. Utilities and their partners (including national laboratories overseen by DOE) will also need to focus on securing that system against efforts to disable or corrupt the flow of data.

Beyond Intelligence Support: Leveraging Government Capabilities to Assist Power Restoration

DHS, DOD, and other federal departments and agencies are rapidly expanding their capabilities to protect and restore critical government networks after a cyber attack on the United States. There is a strong possibility that the president, using Sandy as a precedent, would also direct the federal government to use these capabilities to help utilities restore power if a cyber attack disrupted the grid, especially in areas of extraordinary economic and strategic importance. But the national security context for providing such support in a cyber-induced outage would be entirely different from that created by a hurricane.

As Sandy made landfall, the president told all of his cabinet officers—including Secretary of Defense Leon Panetta—that in addition to supporting FEMA for immediate life-saving operations, the top priority for DOD would be restoring power for lower Manhattan. DOD responded accordingly. Most notably, DOD reallocated C-5A cargo aircraft away from their previously assigned mission to resupply forces in Afghanistan, instead dedicating them to transport utility trucks from West Coast utilities to the New York/New Jersey region.

But the superstorm did not strike any critical military bases or other defense infrastructure. DOD's initial Sandy after-action review noted that the department "dodged a bullet with Sandy: no Defense Critical Assets were degraded." The review also emphasized that in future catastrophes, including those caused by "cyberattacks on critical infrastructure," the department needed to prioritize its ability to ensure the continued execution of its core missions.[82]

A targeted cyber attack, and the political/military crisis that engendered it, would create issues for mission assurance and the allocation of federal cyber response assets above and beyond those created by Sandy. For example, the president might direct DOD (and perhaps even DHS cyber response assets) to prioritize the restoration of mission-essential ICSs and other systems on military bases, especially those important for military operations in the crisis region. Yet, assisting utilities that distribute electricity to those installations would also be a top priority. The same is true of the BES generators, transmission lines, and RTOs that help provide power to those distribution companies. And governors—who are responsible for the public health and safety of their citizens—would surely want to help shape national decision making on power restoration priorities.

Department of Homeland Security Support

The ICS-CERT can provide vital data on threat signatures and mitigation recommendations to support power restoration. What the ICS-CERT does *not* do is put "fingers on the keyboard" of a utility's HMI systems or other OT components to eliminate malware and conduct other power restoration operations. There are good reasons why this is the case. As is true for cross utility mutual assistance,

[81] Patricia Hoffman, letter to Tom Fanning and Fred Gorbet, August 5, 2014, http://www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20%28CRISP%29.pdf.

[82] US Department of Defense, *Talking Points for Deputy Secretary of Defense: Hurricane Sandy After Action Review* (Washington, DC: US Office of the Secretary of Defense, January 10, 2013), 1.

unless OT experts are thoroughly familiar with the systems they are trying to fix, they can accidentally brick those systems in ways that will greatly complicate and delay power restoration.

It might be possible for ICS-CERT teams to partner with specific utilities so that the teams could train on each utility's OT system and develop the deployment plans and operational protocols necessary to help utility personnel conduct malware scrubbing and other hands-on restoration efforts. Staffing and training the ICS-CERT to provide such services to multiple utilities (potentially at the same time in a cyber attack) would require a significant increase in resources. At present, the ICS-CERT is staffed at such a low level that it can only deploy a handful of small fly-away teams simultaneously.[83] Building up these staff assets could provide substantial benefits for power restoration, if utilities and the ICS-CERT can agree on specific high-value support roles that the teams would play beyond their usual responsibilities for forensics assistance and other missions.

Relying on the ICS-CERT to provide such support will also require the resolution of unresolved questions as to whether (and under what circumstances) DHS employees would have the legal authority to directly reconfigure a private utility's ICSs or conduct other operations and what liability exposure the US government might have if such operations fail or go awry. Resolution of these issues should be expedited.

The Department of Energy: Key Authorities and Opportunities to Support Power Restoration

DOE does not maintain fly-away teams equivalent to those maintained in the ICS-CERT program. However, in addition to the lead federal responsibilities that DOE has to support energy restoration under ESF #12, Congress recently granted the department new emergency authorities that could prove enormously significant in responding to cyber attacks on the grid.

On December 4, 2015, President Obama signed into law the Fixing America's Surface Transportation (FAST) Act, which legislates a number of energy security initiatives. One of the provisions, Critical Electric Infrastructure Security, provides that when directed by the president, the secretary of energy can "issue such orders for emergency measures as are necessary . . . to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure" (i.e., infrastructure serving US facilities "critical to the defense of the United States" and other facilities as designated by the secretary of energy).[84] The legislation does not specify which particular actions the secretary might take within this grant of authority. Rather, Congress required that within 180 days of enactment of the bill, the secretary establish rules of procedure that ensure that such authority can be exercised expeditiously.[85]

As the secretary meets this requirement, DOE might coordinate with the electric industry not only on the procedures for issuing emergency orders but also on the types of orders that might be most valuable in the prioritized sustainment and restoration of power in a cyber event. As noted in the discussion of CONOPS for power restoration, the power industry could face significant issues in terms of whether to segment the grid and intentionally create power islands in a large-scale outage. Traditional imperatives to quickly restore power might also conflict with requirements to take grid components off-line to limit the spread and reduce the consequences of an attack. As the electric subsector examines potential restoration CONOPS and federal leaders consider measures for prioritized sustainment and restoration for defense

[83] Information provided by DHS to the author, November 3, 2015.

[84] Fixing America's Surface Transportation (FAST) Act, H.R.22, 114th Cong. (2015–2016), Section 61003, "Critical Electric Infrastructure Security," 806–807, https://www.congress.gov/bill/114th-congress/house-bill/22/text#toc-HDB4083C95A7D42688DE939127F01DF82.

[85] FAST Act.

critical electric infrastructure, close collaboration between industry and government leaders on such FAST Act implementation-related issues will be vital.

Department of Defense Capabilities: Assistance from US Cyber Command?

When President Obama met with his cabinet after Sandy made landfall and he emphasized that support for power restoration was an overriding priority for federal departments, department leaders heard his message loud and clear. But many of those departments—including DOD—had never before considered restoration of the US grid a priority mission, and they scrambled with their interagency partners to do the best they could to identify appropriate support missions and assets.

In a severe blackout caused by a cyber attack, it is possible that the president will once again turn to the secretary of defense and direct that DOD support power restoration operations. That possibility will be especially strong if the attack jeopardizes the flow of electricity to critical national security installations, including those necessary for commanding, controlling, and resupplying forces in the regional confrontation that sparked the attack. DOD, its interagency partners, and the electric industry must prepare for this eventuality and ensure that DOD assistance for post-cyber attack power restoration directly supports industry needs.

Planning for such defense support is very much a work in progress. *The DoD Cyber Strategy* (2015) provides a foundation for assessing potential DOD roles in a cyber attack on the US power grid and other critical infrastructure sectors. The strategy notes that during a conflict, adversaries may seek a strategic advantage by targeting utility ICSs and other infrastructure components.[86] The strategy also states that "DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence," which may include "loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[87] A nationwide cyber attack on utilities targeted for maximum political, military, and economic consequences would almost certainly rise to that level.

The strategy notes that, if directed by the president or secretary of defense, the US military may conduct cyber operations to blunt an attack and prevent the destruction of property or loss of life.[88] Such operations could occur both at home and abroad (including the disruption of an adversary's "military-related critical infrastructure").[89] The document does not, however, specifically address whether and how DOD might help utilities scrub malware from their networks or conduct other power restoration operations. Instead, the strategy provides a road map to advance the consideration of possible support missions but leaves key issues still to be resolved.

One issue is how DOD would provide assistance as part of the federal team. During Sandy, when President Obama told the secretary of defense that power restoration would be a top DOD priority, he added a key condition: FEMA and DHS would remain the lead federal agencies in charge of coordinating federal disaster response operations. DOD would operate strictly in support of civil authorities, rather than exercising any leadership using its own Title 10 or other authorities for homeland defense. The Defense Support of Civil Authorities operations that followed during Sandy included both support for power restoration and assistance in dealing with the consequences of the outage for public health and safety.

[86] US Department of Defense, *The DoD Cyber Strategy* (Washington, DC: US Department of Defense, April 2015), 2, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[87] Ibid., 5.

[88] Ibid.

[89] Ibid., 14.

A similar approach could be adopted for defense support in a cyber attack. *The DoD Cyber Strategy* calls for the department to "develop a framework and exercise its Defense Support of Civil Authorities (DSCA) capabilities in support of DHS and other agencies and with state and local authorities to help defend the federal government and the private sector in an emergency if directed." To help meet that exercise requirement, the department's Cyber Guard exercise focuses on contingencies that may require emergency allocation of DOD forces to help protect critical infrastructure under the leadership of other federal agencies.[90] Cyber Guard exercises are now conducted annually and include electric utilities as participants.

Admiral Michael S. Rogers, Commander, USCYBERCOM, emphasizes the value of Cyber Guard for advancing a shared understanding of how defense support might be provided in a cyber attack:

> We inaugurated the CYBER GUARD exercise series to test the "whole of nation" response to a major cyber incident affecting the DoDIN [Department of Defense Information Network] and U.S. critical infrastructure. USCYBERCOM offices work with experts from the Joint Staff and the joint cyber headquarters elements, Cyber Mission Force teams, U.S. Northern Command, National Guard, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), state governments, allies, and the private sector. Our defenders battle in the exercise networks against a world class "opposing force" to make this nearly three-week event as realistic as possible. The idea is to train our forces to operate as they would in an actual cyber crisis—i.e., against live opposition and alongside the federal, state, allied, and industry partners who would also have authorities and equities in such an event. Over a thousand participants, including representatives from critical infrastructure partners and National Guard teams from 16 states, practice how to collectively protect the nation along with DoD networks. Participants from the Department of Defense practice lending appropriate support to civil authorities, and doing so on a complex exercise network that takes months to fine tune in advance of CYBER GUARD.[91]

However, major issues remain to be resolved in terms of identifying specific capabilities that DOD would be prepared to bring to bear in support of DHS for power restoration. USCYBERCOM is building a Cyber National Mission Force that could have substantial capabilities to meet utility RFAs, as coordinated and assigned by DHS and approved by the secretary of defense. In particular, because the Cyber Protection Team (one of three components of the overall Cyber National Mission Force) is responsible for defending DOD networks and ICSs, it is likely to have technical expertise and deployable assets that might be useful for post-cyber attack power restoration.[92]

But the Cyber Protection Team is responsible for securing and restoring DOD systems. Whether the force could be diverted from its DOD mission to support the private sector, especially at a time when DOD assets are at risk of attack, will present a continuing policy challenge. The extent to which DOD forces can operate on utility systems by leveraging the authorities of DHS or other federal departments and agencies also presents unresolved issues.

An additional problem lies in specifying the tasks that USCYBERCOM personnel would perform to

[90] Ibid., 22.

[91] *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong. (September 29, 2015) (statement of Admiral Michael S. Rogers, Commander, US Cyber Command), 4–5, http://www.armed-services.senate.gov/imo/media/doc/Rogers_09-29-15.pdf.

[92] Cheryl Pellerin, "Rogers: Cybercom Defending Networks, Nation," *DoD News, Defense Media Activity* (August 18, 2014), http://www.defense.gov/news/newsarticle.aspx?id=122949.

support power restoration. The same constraints that limit the ability of utilities to work on each other's OT systems, which differ significantly in terms of system designs, applications, and other technical features, will also apply to military forces. Providing the utility-specific training and exercising opportunities for full-time military personnel on Title 10 status will be especially difficult. Far more promising is the possibility of providing such training for state National Guard personnel.

National Guard

The pace of power restoration after Sandy was greatly accelerated by the support missions performed by state National Guard organizations and other government agencies. Key missions and implications for post-cyber attack restoration include the following:

- ***Logistics support for restoration crews:*** During Sandy, state National Guard and DOD installations served as staging sites and base camps for utility crews providing mutual aid. By providing housing, food, and vehicle refueling and meeting the other support needs for crews from as far away as Canada, Arizona, and California, this logistical assistance was a critical enabler for industry's mutual aid system and will remain critical after other natural disasters. In contrast, large-scale logistical support will be less necessary for the specialized remediation tasks required for post-cyber attack restoration.
- ***Engineering support:*** Debris and road clearance proved crucial after Sandy for giving utility crews access to damaged grid infrastructure. These efforts, along with emergency evaluation of physical damage to bridges and other structures, will be essential after future natural hazard events of similar or greater severity. However, cyber events will not require these traditional engineering support functions.
- ***Public safety/security:*** After Sandy, utility contractors, state and local law enforcement, National Guard personnel, and other partners provided for wire guarding (site safety), flagging (traffic control), and other safety/security-related support missions. Again, cyber events will not typically necessitate such restoration support, although long-duration power outages could jeopardize public health and safety and therefore require substantial Guard resources to meet those challenges.
- ***Situational awareness:*** Utilities have substantial experience in mapping their outage areas and are currently using smart metering and other grid modernization tools to more rapidly identify where repairs are needed. As the federal lead for ESF #12, Energy, DOE attempted to support these restoration efforts by providing broader situational awareness of the availability of fuel for response vehicles and choke points in the broader flow of energy resources, as well as other types of data. DOE's after-action review of Sandy found that significant improvements are needed to provide shared real-time situational awareness of damage to the grid and associated energy infrastructure, as well as in refining estimated times of restoration (ETRs) and coordinating communication of these times to communities and government leaders.[93] An equivalent system will be required for cyber attacks. However, such a system will also have to account for the risk that the adversary will corrupt situational awareness data and the networks over which data travel.

DOE, the National Guard, and their industry partners are making significant improvements in situational awareness tools and technologies. These initiatives could provide a basis to help utilities better understand the scope and failure nodes in a cyber event if attackers disrupt their usual sources of data for making such assessments. National Guard efforts

[93] US Department of Energy, *Overview*, 7-1.

to develop advanced geospatially based displays for critical infrastructure assessments (tailored to be shared with industry) may be especially useful.

Most important, many National Guard organizations are building on their long-established support relationships with utilities in their states and are developing the sorts of utility-specific training and operational plans that could enable Guard personnel to directly support post-cyber attack restoration operations. California provides a case in point. In August 2015, Governor Jerry Brown issued an executive order to establish a Cyber Incident Response Team to partner with the private sector to support cyber threat detection, reporting, and response operations.[94] National Guard organizations in Washington State, Maryland, South Carolina, Michigan, and many other states are aggressively moving forward with their utility partners to advance similar restoration initiatives.[95]

Of course, plans for Guard assistance will be useless unless the Guard and its partners can train and exercise the pool of personnel needed to help utilities restore power after a cyber attack. The Cyber Guard exercise provides some training but only occurs once a year. The Army National Guard's annual response exercise, Cyber Shield, provides additional training and hands-on response simulations that have included students from the Guard and Title 10 Reserve personnel sitting alongside students employed by power utilities. Most notably, Cyber Shield has begun using a virtual cyber city that facilitates realistic training on power grid defense and restoration.[96] The continued development and expansion of training simulation tools will be essential to achieve the throughput needed by the National Guard, Reserves, and the utilities they will support. Development of detailed student assessment tools to measure the effectiveness of such training (and to support skill certification initiatives) will also be essential.

However, beyond providing foundational OT defense and restoration skills, preparing personnel to help restore the utility-specific ICSs will remain a challenge. Dozens of states have part-time National Guard personnel who also work for cyber-related firms. Guard leaders in Washington State, Maryland, and a growing number of other states are partnering with their local utilities to explore how these cyber-skilled personnel might provide a surge force to support power restoration operations. Another promising option proposed by an officer in the Maryland National Guard is that National Guard personnel would maintain their primary (full-time) civilian employment with electric utilities and other critical infrastructure entities while also maintaining part-time membership in the National Guard where they would receive specialized, classified training.[97]

If utilities were to hire such National Guard personnel to help operate their OT systems (or if existing utility employees were to join the National Guard), the familiarity of these personnel with proprietary software and other features of utility systems would enhance their ability to effectively restore power and put "hands on the keyboard." However, the National Guard Bureau and its partners in DOD need to continue to clarify the extent to which National Guard forces can conduct such hands-on activities in either Title 32 or Title 10 status and where additional authorities may be needed through legislative action. The ability of these National Guard forces to help defend utility networks while under state active duty,

[94] Exec. Order No. B-34-15, 3 C.F.R. (2015).

[95] See, for example, State of Michigan Executive Office, *Michigan Cyber Disruption Response Strategy* (Lansing, MI: State of Michigan Executive Office, September 16, 2013), https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.

[96] Jessica Cates, "Cyber Shield Concluded in Admiration," *Atterbury Muscatatuck*, March 27, 2015, http://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/TabId/582/artmid/4756/articleid/25/Cyber-Shield-Concluded-in-Admiration.aspx.

[97] Victor R. Macias, "Game Changing Pivot" (master's thesis, University of Maryland Baltimore County, 2015), 14–17.

consistent with the laws and constitutions of their respective states and under the command of their governors, will need state-specific analysis as well.

Utilities seeking to rely on support from state National Guard personnel may also be in for a harsh surprise when an attack occurs: those personnel may be assigned to other duties. In periods of heightened risk of cyber attack, governors may place their National Guard forces on state active duty to help restore state IT networks and other non-utility assets. State National Guard forces may also be federalized (that is, put into Title 10 status) to serve national priorities. Indeed, significant elements of the National Mission Team workforce for USCYBERCOM may ultimately be composed of National Guard force personnel.[98] Before an attack occurs, it will be essential to deconflict these potentially competing demands on the National Guard and clarify in advance which personnel will be available to support power restoration.

Allocating Government Assistance: Coordinating Mechanisms and Criteria for Prioritization

Even during Sandy, when mutual assistance assets were plentiful and tens of thousands of National Guard and other state and federal agency personnel were available to support restoration operations, significant problems emerged in the allocation of resources to meet utility RFAs. Industry and its government partners have aggressive, far-reaching efforts under way to fill those gaps for natural hazards. The following analysis draws cyber-related lessons learned from shortfalls during Sandy and describes the ongoing improvements to address them.

The Request for Assistance Process: Lessons from Sandy

Sandy and the Broader Disaster Response System

The process for allocating government support capabilities had the benefit of being based on a rock-solid foundation: that of the NRF. The NRF provides well-established guidelines for traditional disaster-response operations, including the following:

- Fundamental, doctrinal principles to guide, structure, and integrate response efforts across all levels of government and for government to coordinate with nongovernmental organizations and private sector partners.[99] In particular, the NRF is aligned closely with the National Incident Management System (NIMS), which provides the incident management system on which the framework relies and specifies the command-and-control arrangements for disaster responders.[100]
- Specific emergency support functions and (together with the *National Preparedness Goal*) core capabilities required for each function, including transportation, communications, and energy[101]
- Clear descriptions of the roles and responsibilities of federal departments and agencies, including the lead federal organization for each specific aspect of disaster response[102]
- Explicit recognition of the leading role that governors play in requesting federal assistance and the basic process by which FEMA will provide

[98] Sydney J. Freedberg, "National Guard Fights for Cyber Role in 2015 Budget," *Breaking Defense*, February 5, 2014, http://breakingdefense.com/2014/02/national-guard-fights-for-cyber-role-in-2015-budget/.

[99] US Department of Homeland Security, *National Response Framework*.

[100] Ibid., 3–4, 30–33.

[101] Ibid., 31–36; and Department of Homeland Security, *National Preparedness Goal*, 1st ed. (Washington, DC: US Department of Homeland Security, September 2011), http://www.fema.gov/pdf/prepared/npg.pdf.

[102] US Department of Homeland Security, *National Response Framework*, 31–38.

mission assignments to federal agencies through the RFA system

The NRF has a strong grounding in US statutes that further minimize the risk that agencies will misunderstand their roles, responsibilities, and sources of funding in assisting power restoration and other disaster response operations. In particular, the Stafford Act provides "triggers" and thresholds for federal support activities and reimbursement mechanisms for disaster-response operations; in addition, it authorizes the federal government to conduct specific disaster preparedness and response activities, including the traditional restoration support missions conducted by National Guard in state active duty (and funded as authorized by the Stafford Act).[103]

The NRF also offers the advantage of being thoroughly familiar to and respected by agencies at all levels of government. Every federal department with significant roles in disaster response trains to operate within the guidelines of the NRF, NIMS, and associated plans and doctrine. The same is true of state emergency management agencies that help governors generate RFAs. Moreover, federal and state agencies—and with increasing frequency, utilities and other infrastructure owners and operators—collaborate on dozens of exercises and other capacity-building events every year to ensure they can effectively operate within the NRF. One additional factor helps facilitate these exercises and the broader familiarity with how support for utilities can go forward under the NRF: the framework is entirely unclassified.

Leveraging the *National Response Framework* for Power Restoration

Although the NRF is designed to encompass all hazards and provides a strong foundation for managing the consequences of cyber attacks (including those on public health and safety), the Obama administration has advanced an additional effort to coordinate government and private sector responses to cyber events.[104] DHS issued the interim *National Cyber Incident Response Plan* (NCIRP) in 2010 as an initial step to provide for such coordination. The interim plan lacks many of the advantages of the NRF and is poorly aligned with it. The analysis that follows identifies key problems in the interim NCIRP that should be remedied in a new cyber incident response framework and recommends how lessons learned from using the NRF during Sandy might be applied in response operations.

Shortfalls in the Interim *National Cyber Incident Response Plan*

The interim NCIRP establishes a "strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident," including critical infrastructure restoration operations.[105] The drafting of that document marked a vital first step toward meeting the challenges of responding to a cyber attack. Yet, recent exercises have identified significant shortfalls and ambiguities in the NCIRP strategic framework. The National Level Exercise (NLE) 2012,[106] which simulated a far-reaching cyber attack on SCADA networks and other critical

[103] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288, as amended, 42 USC. 5121 et seq.

[104] In addition to the NRF itself, the Bush administration issued a now-outdated 2004 annex, "Cyber Incident," to the framework. US Department of Homeland Security, "Cyber Incident Annex," in *National Response Framework*, http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf.

[105] US Department of Homeland Security, *National Cyber Incident Response Plan*, interim version (Washington, DC: US Department of Homeland Security, September 2010), 1, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

[106] For more information, see "National Level Exercise 2012: Cyber Capabilities Tabletop Exercise," FEMA, https://www.fema.gov/media-library/assets/documents/26845.

infrastructure components, identified several key areas for improvement:

- Doctrinal and structural challenges, including time-consuming decision processes and an inability to generate viable, prioritized action plans. FEMA's report on the exercise found that "the multiple layers of coordination for cyber incidents confused participants and contributed to slow decision-making relative to the speed of the evolving cyber campaign."[107]
- Problems in accessing certain critical capabilities, including an inability to provide or procure the technical resources necessary to meet RFAs
- Ambiguities in the roles and responsibilities of various response agencies, including a lack of detail on the functions of response organizations, including those assigned to the National Cybersecurity and Communications Integration Center, the staff and senior levels of the Unified Coordination Group, the Domestic Resilience Group, the Cyber Response Group, law enforcement, and private sector owners and operators of critical infrastructure
- Uncertainties over the statutory authority for federal assistance, including how the Stafford Act might authorize federal support activities and reimbursement efforts after a cyber attack[108]

In developing a National Cyber Incident Response Framework (NCIRF) to replace the interim plan, DHS and its interagency partners will need to resolve each of these problems. However, government agencies alone will be unable to do so. Input from—and collaboration with—electric utilities and other critical infrastructure sector owners and operators will be essential to design a framework that can help them accelerate service restoration and quickly respond to industry priorities for assistance.

The NLE findings did not address an additional shortfall in the interim plan: the failure to assign governors an appropriate role in requesting federal assistance after a cyber attack and in helping to oversee response operations. Governors have primary responsibility in their states for public health and safety, both of which can be jeopardized by major power outages regardless of their cause. During Sandy, Governor Cuomo, Governor Christie, and other governors in the region were intensely focused on restoration operations for the grid and other critical infrastructure sectors. Consistent with the NRF, the governors took the lead in requesting and prioritizing federal assistance during the storm. The governors and their adjutant generals played a key role in allocating scarce National Guard resources to support utilities in restoring power. Of course, the involvement of governors in a multistate event adds a degree of political complexity to response operations, especially in the allocation of scarce federal resources and in shaping public messaging on restoration time lines and other sensitive issues.[109] That complexity is inherent in the constitutional structure of the United States and is just another coordination challenge in responding to major disasters.

Governors and federal department leaders are now exploring how to plan for such coordinated action in cyber attacks on the grid. The Council of Governors is driving that effort forward. Formally established by President Obama on January 11, 2010, the council enables governors to address issues involving the National Guard, homeland defense, and Defense Support to Civil Authorities with the leadership of

[107] FEMA, *National Level Exercise 2012: Quick Look Report* (Washington, DC: Department of Homeland Security, March 2013), 12, http://www.fema.gov/media-library-data/20130726-1911-25045-9856/national_level_exercise_2012_quick_look_report.pdf.

[108] Ibid.

[109] Susanne Craig, "Cuomo's Role in Hurricane Sandy Inquiry Foretold Fate of His Ethics Panel," *New York Times*, October 30, 2014, http://www.nytimes.com/2014/10/30/nyregion/cuomos-role-in-hurricane-sandy-inquiry-foretold-fate-of-his-ethics-panel.html?_r=0.

FEMA, DHS, DOD, and the White House.[110] The council and its federal participants have adopted the *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (2014), which provides a "framework for establishing a collaborative environment for States, territories, and the Federal government to expedite and enhance the nation's response to cyber incidents."[111]

The unity of effort initiative is specifically targeted to help resolve the issues of authorities and mission deconfliction that will otherwise impede effective post-cyber attack power restoration. To make the effort still more valuable, DOE and representatives of the electricity sector should also be brought into the response planning now under way.

Building a Cyber Response Framework: Lessons Learned from Employing the *National Response Framework* during Sandy

Although the NRF is a model of clarity, and federal departments and their sponsors had years of experience in functioning under it in events before Sandy, the scale of assistance operations required by the superstorm—and the specific RFAs that stemmed from utility power restoration operations—produced major lessons for developing and implementing a cyber response framework.

In its after-action report for Sandy, DOE noted that because of the size of Sandy and the uncertainty in where severe impacts would occur, utilities throughout the region retained crews in their own service territories as a necessary precaution. As the storm progressed northward, utilities had to assess, repair, and certify their own systems before releasing crews to areas where the storm continued to impact the electric infrastructure. Similar problems could emerge in a cyber attack on utility systems.[112]

DOE also found that during Sandy, the movement of crews and equipment within the region and within states was not adequately communicated and coordinated with state and local governments. In many cases, "states were not aware of the processes and protocols of the existing mutual aid framework which led to confusion at the local level as crews transited impacted areas."[113] Equivalent problems are likely to emerge in a targeted cyber attack and should be taken into account in designing and operating the NCIRF.

Finally, DOE emphasized the benefits of having dedicated senior leaders involved in shaping response operations. DOE found that the scale of Sandy's impact required direct CEO involvement in hurricane response, as well as direct and regular communication between CEOs and federal and state leaders. For example, the secretary of energy and governors participated in daily conference calls with CEOs of major utility companies to assess electricity restoration and conditions. These communications both aided the restoration process and provided situational awareness to the government, enabling increased coordination between the public and private sectors. Additionally, the high-level interactions led to the placement of a private sector staff at the FEMA National Response Coordination Center (NRCC). This facilitated greater access to services and resources to support restoration. Senior leaders in the field also provided senior management at DOE headquarters with high-level situational awareness.[114]

This finding has major implications for designing and operating a cyber response framework to support

[110] Exec. Order No. 13528 ("Establishing Council of Governors") (January 11, 2010), https://www.whitehouse.gov/the-press-office/president-obama-signs-executive-order-establishing-council-governors.

[111] Council of Governors, *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (Washington, DC: National Governors Association, July 2014), http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

[112] US Department of Energy, *Overview*, 9.

[113] Ibid.

[114] Ibid., 6.

power restoration. Dedicated CEO-level participation by utilities will be essential to prioritize and shape government assistance operations. In the aftermath of Sandy, the ESCC has been formalizing procedures for CEO involvement in power restoration decisions; those efforts should be leveraged for cyber response. DHS, its federal partners, and the private sector should also assess the advantages of continuing to leverage FEMA's NRCC as an all-hazards venue for allocating and coordinating federal assistance operations, versus creating a separate cyber-only system.

Beyond Immediate Response Operations: Follow-on Phases of Power Restoration and "Grid Reconstitution"

When an adversary launches a coordinated cyber attack against multiple US utilities, power restoration operations will go forward in sequential phases. The NERC report *Severe Impact Resilience: Considerations and Recommendations* (2012) outlines a three-phased process that would occur in the aftermath of a catastrophic cyber attack on the grid.

The initial "mitigation" phase in a catastrophic outage would occur during the first days of the event and would include immediate power restoration operations. The second phase, a "new normal" period, would follow and last multiple weeks or even longer. Reattacks could occur during this new normal period and generation would remain inadequate to serve all consumer loads. The third phase would be marked by the electric system's return to normal service and reliability.[115]

Phases One and Two in a Targeted Attack

An equivalent three-phase sequence would occur in response to the less-catastrophic selectively targeted attack scenario examined in this study. However, the initial mitigation phase in a targeted attack would require restoration tasks and priorities beyond those cited in the NERC report. For example, if adversaries attempt to cut off power to critical US defense installations, and thereby disrupt their ability to conduct operations in an escalating regional crisis, prioritizing the restoration of power to those installations would be essential. Strengthening emergency power capabilities at such installations and partnering with the electric industry to improve their energy resilience could also provide a vital hedge against cyber attacks. These efforts could be extended to critical national security installations nationwide and supported by new industry–government partnership models and cost recovery mechanisms that can underwrite utility investments in cyber resilience.[116]

A targeted attack would also require specialized public messaging strategies and exceptionally close coordination by utility CEOs and government leaders in communicating with affected citizens. In weather-induced blackouts, the ETRs that utilities communicate to the public are often the focus of intense scrutiny by customers, elected officials, and the media. Establishing unity of messaging on ETRs between power companies and government leaders can help them manage public expectations and support disaster response planning and operations.

A cyber attack will present more challenging communications issues than natural hazards will, both in terms of the goals to be achieved and in the technical difficulties of providing accurate, consistent messages to the public. Adversaries are likely to launch targeted cyber attacks to achieve specific political and military effects. To advance their goals, they may seek to magnify the public's uncertainties

[115] Ibid., 14–16.

[116] Especially important in this regard, DOD is analyzing potential gaps in energy resilience in defense installations and investigating new business models that might facilitate expanded public-private partnerships to strengthen such resilience. US Department of Defense, *Energy Resilience Business Case Analysis Study*.

and concerns about the duration of cyber-induced outages and foment doubt regarding the ability of the US government to preserve the safety and security of its citizens.

US government and industry messaging will need to be designed and coordinated to counter such efforts. Communications with the public will need to account for the risk of reattacks on distribution systems that have been restored to service and the possibility that other regions may be attacked after initial restoration operations are under way. Government and industry leaders should also be prepared to explain potentially controversial restoration decisions (including the possibility of grid segmentation) that may be undertaken in restoration phases one and two. To the extent that restoration playbooks and CONOPs preplan for such options, those plans should include strategic messaging components that can be exercised along with other restoration activities.

Phase Three: Grid Reconstitution

According to the NERC report, the third phase of power restoration would be marked by the electric system's return to normal service and reliability. However, the post-cyber attack power grid will be significantly different from what it was before the initial attack. Utilities will have adopted effective protection and mitigation measures against the cyber weapons used by the adversary and will already be implementing lessons learned from the event to strengthen mutual assistance in the future.

The attack will also create both the impetus and the political opportunity for much more far-reaching changes. Just as occurred after 9/11, when al-Qaeda's attack spurred Congress and the Bush administration to adopt policies and organizational changes (including the creation of DHS) that they had previously refused to support, a cyber attack on the grid that successfully disrupts critical functions and services during a crisis will open the door to changes in the grid architecture and resilience characteristics that are now considered too politically difficult, technologically challenging, or expensive. In short: utilities and their partners will have a unique opportunity to reconstitute the grid and shift it toward a more inherently resilient structure.

Now is the time to plan for such an opportunity. In addition to accelerating the voluntary implementation of the NIST framework and other resilience recommendations developed in partnership with industry, government agencies and the private sector could also identify ambitious goals that anticipate (and ideally, get ahead of) future increases in the threat. Patricia Hoffman, the DOE's assistant secretary for the Office of Electricity Delivery and Energy Reliability (OE), has suggested a number of initiatives that might contribute to a grid reconstitution plan. One is to develop "out-of-band" technologies to monitor critical grid operations that cannot be attacked by cyber adversaries. Another is to adopt much more aggressive and far-reaching supply chain risk management policies and programs than are practical today.[117]

Given the risk that adversaries will seek to disrupt the utility communications systems on which power restoration will depend, utilities should also continue to explore initiatives to strengthen the resilience of their communications systems against cyber attack. Such measures might include the development of utility-owned and -maintained fiber optic communications. The development of last-mile technologies that can create more difficult-to-bridge gaps for cyber attackers to cross may be equally important for reconstitution strategies. Federal funding to support

[117] Pat Hoffman, "Plenary" (lecture, Resilience Week 2015 Conference, August 20, 2015, Philadelphia, PA). The RADICS initiative supports the development of a number of such initiatives, including "out-of-band" situational awareness technologies, secure emergency networks to provide communications during restoration operations, and automated threat analysis. Defense Advanced Research Projects Agency, *Broad Agency Announcement: RADICS*, 7–12.

such research and development efforts may need to be increased accordingly.[118]

It would be even better if these far-reaching improvements could be adopted before an adversary strikes. Improving the grid's resilience may even help reduce the likelihood of such an attack by increasing an adversary's uncertainty as to whether the benefits of attacking the grid would be worth the potential costs of US retaliation. However, until deterrence is certain to prevent cyber attacks on the US power grid, measures to accelerate power restoration if an attack occurs will be vital.

Conclusion

Sandy and other severe natural events have helped the electricity sector forge an impressive power restoration system for such hazards. Efforts to strengthen resilience against cyber attacks must go forward without the benefit of such real-world experience and will have to account for strikingly different restoration challenges. Nevertheless, rather than build a separate cyber-specific restoration system from scratch, utilities and their partners should pursue opportunities to adapt the existing system to meet cyber threats as well.

The first step will be to establish a design basis for post-cyber attack power restoration. Major uncertainties persist regarding the effects that cyber attacks can inflict on the grid, both because the future capabilities of adversaries are so difficult to determine and because power companies and their research partners are accelerating the development of new resilience measures. To help conduct an analysis of alternatives to determine which resilience investments are most cost effective and how they should be supported with new restoration training initiatives and exercises, it will be important to further refine our understanding of the physical damage, cascading outages, and other disruptive effects that potential adversaries will be able to create.

However, based on the targeted attack scenario described in this study, key challenges and opportunities to structure a post-cyber attack restoration system are already evident. Further exercises and collaborative planning efforts will be essential to help utilities overcome the disincentives for sharing restoration assets in cyber events. A crawl, walk, run approach to cross utility assistance may offer the most promise to build the talent pool for mutual aid and meet the technical challenges of restoring utility-specific ICSs.

Building a CONOPS to guide restoration operations will also be vital. Such a CONOPS will need to address the unique challenges of cyber threats, versus those of natural hazards, and will require supporting energy management and communications systems that can survive attacks targeted on them. Government partners can play a key role in helping industry develop and implement a cyber CONOPS. In particular, these partners may be able to provide tightly coordinated threat and remediation data to industry to support power restoration while utilities themselves lead the hands-on restoration of their own networks and grid components.

Further analysis will be required to determine whether and how DHS, the National Guard, and other potential sources of government support could provide such hands-on assistance if requested by utilities. Yet, any such assistance should be provided in ways that are consistent with the NRF and other proven, effective mechanisms for responding to RFAs. Future cyber response frameworks might be structured accordingly and used as part of the starting point to conduct an analysis of alternatives for potential government and private contractor sources of assistance to utilities.

Ultimately, however, mutual assistance between utilities will likely offer a crucial means for power

[118] Assante, Roxey, and Bochman, *The Case for Simplicity*, 6–7.

companies to supplement their own restoration capabilities. Creating the training, exercise, and governance system necessary for such assistance before a cyber attack occurs will be vital for saving lives and defending the United States if adversaries strike—and for making the grid a less tempting target in future crises.

Bibliography

All Hazards Consortium. *The Multi-State Fleet Response Initiative Working Group Workshop Report: Rapid Critical Infrastructure Restoration through Joint Integrated Planning for the Movement of Private Sector Resources in Response to Hurricane Sandy.* Frederick, MD: All Hazards Consortium, January 2013. http://www2.apwa.net//Documents/About/TechSvcs/Multi-stateFleetResponseWorkshopReport-02-21-13.pdf.

Allison, Phillip. "Cloak and Secure Your Critical Infrastructure, ICS and SCADA Systems: Building Security into Your Industrial Internet." Paper presented at Pacific Northwest Section American Water Works Association Conference, Bellevue, WA, 2015. http://www.pnws-awwa.org/uploads/PDFs/conferences/2015/Technical%20Sessions/Thursday/4_Cloak%20and%20Secure%20Your%20Critical%20Infrastructure,%20ICS%20and%20SCADA%20Systems.pdf.

Assante, Michael J., 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.

Assante, Michael, Tim Roxey, and Andrew Bochman. *The Case for Simplicity in Energy Infrastructure: For Economic and National Security*. Washington, DC: Center for Strategic and International Studies, November 2015. http://csis.org/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf.

Atkinson, William. "Mutual Aid Comes of Age." *Public Power* 70, no. 2 (March–April 2012), http://www.publicpower.org/Media/magazine/ArticleDetail.cfm?ItemNumber=34001.

Bea, Keith, L. Cheryl Runyon, and Kae M. Warnock. *Emergency Management and Homeland Security Statutory Authorities in the States, District of Columbia, and Insular Areas: A Summary.* CRS RL32287. Washington, DC: Congressional Research Service, 2004.

Bipartisan Policy Center. *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, A Report from the Co-Chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative.* Washington, DC: Bipartisan Policy Center, February 2014. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

Cates, Jessica. "Cyber Shield Concluded in Admiration." *Atterbury Muscatatuck*, March 27, 2015. http://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/TabId/582/artmid/4756/articleid/25/Cyber-Shield-Concluded-in-Admiration.aspx.

Clapper, James R. *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*. 114th Cong., September 29, 2015. http://www.armed-services.senate.gov/imo/media/doc/Clapper_09-29-15.pdf.

Connecticut Public Utilities Regulatory Authority. *Cybersecurity and Connecticut's Public Utilities*. New Britain, CT: Connecticut Public Utilities Regulatory Authority, April 14, 2014. http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.

Constantin, Lucian. "Attack Campaign Infects Industrial Control Systems with BlackEnergy Malware." *PCWorld*, October 29, 2014. http://www.pcworld.com/article/2840612/attack-campaign-infects-industrial-control-systems-with-blackenergy-malware.html.

Council of Governors. *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity.* Washington, DC: National Governors Association, July 2014. http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

Craig, Susanne. "Cuomo's Role in Hurricane Sandy Inquiry Foretold Fate of His Ethics Panel." *New York Times*, October 30, 2014. http://www.nytimes.com/2014/10/30/nyregion/cuomos-role-in-hurricane-sandy-inquiry-foretold-fate-of-his-ethics-panel.html?_r=0.

Critical Infrastructure Partnership Advisory Council. "Electricity Subsector Coordinating Council and Government Executives Meeting Agenda," June 15, 2015. https://www.dhs.gov/sites/default/files/publications/cipac-elec-scc-govt-exec-agenda-06-15-15-508.pdf.

Danzig, Richard J. *Preparing for Catastrophic Bioterrorism: Toward a Long-Term Strategy for Limiting the Risk.* Defense & Technology Paper. Washington, DC: Center for Technology and National Security Policy, May 2008. http://ctnsp.dodlive.mil/files/2014/10/Preparing-for-Catastrophic-Bioterrorism.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. http://www.cnas.org/surviving-diet-poisoned-fruit#.VqvPFkajYgk.

Defense Advanced Research Projects Agency. *Broad Agency Announcement: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)*. DARPA-BAA-16-14. Arlington, VA: Defense Advanced Research Projects Agency, December 11, 2015. https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-16-14/listing.html.

Defense Science Board. *Task Force Report: Resilient Military Systems and the Advances Cyber Threat*. Washington, DC: Defense Science Board, January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

Donovan, Shaun. "Hurricane Sandy Rebuilding Strategy: Helping Communities Prepare for the Impacts of a Changing Climate." *The White House* (blog). August 19, 2013. https://www.whitehouse.gov/blog/2013/08/19/hurricane-sandy-rebuilding-strategy-helping-communities-prepare-impacts-changing-cli.

Edison Electric Institute. *Before and after the Storm: A Compilation of Recent Studies, Programs, and Policies Related to Storm Hardening and Resiliency, Update*. Washington, DC: Edison Electric Institute, March 2014.

———. *Mutual Assistance Enhancements*. Washington, DC: Edison Electric Institute, October 2013. http://www.eei.org/issuesandpolicy/RES/TAB%205.pdf.

———. "Spare Transformers." http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

Electric Infrastructure Security Council (2014). Electric Grid Protection (E-PRO) Handbook.

Emergency Management Assistance Compact website, http://www.emacweb.org/.

Executive Order No. 13528.

Executive Order No. B-34-15, 3 C.F.R. 2015.

Fenton, Robert. *Defense Support of Civil Authorities: A Vital Resource in the Nation's Homeland Security Missions: Written Testimony Before the House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications*, 114th Cong., June 10, 2015. http://www.dhs.gov/news/2015/06/10/written-testimony-fema-house-homeland-security-subcommittee-emergency-preparedness.

Finkle, Jim. "Exclusive: Insiders Suspected in Saudi Cyber Attack." *Reuters*, September 7, 2012. http://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907.

Fixing America's Surface Transportation (FAST) Act. H.R.22, 114th Cong. (2015–2016). https://www.congress.gov/bill/114th-congress/house-bill/22/text#toc-HDB4083C95A7D42688DE939127F01DF82.

Freedberg, Sydney J. "National Guard Fights for Cyber Role in 2015 Budget." *Breaking Defense*, February 5, 2014. http://breakingdefense.com/2014/02/national-guard-fights-for-cyber-role-in-2015-budget/.

Fugate, Craig. *Improving the Nation's Response to Catastrophic Disasters: How to Minimize Costs and Streamline our Emergency Management Programs: Hearing Before the United States House Transportation and Infrastructure Committee, Subcommittee on Economic Development, Public Buildings, and Emergency Management*. 112th Cong., March 30, 2011. http://www.fema.gov/pdf/about/programs/legislative/testimony/2011/3_30_2011_improving_the_nations_response_to_catastrophic_disasters.pdf.

Hakim, Danny, Patrick McGeehan, and Michael Moss. "Suffering on Long Island as Power Agency Shows Its Flaws." *New York Times*, November 13, 2012. http://www.nytimes.com/2012/11/14/nyregion/long-island-power-authoritys-flaws-hindered-recovery-efforts.html?_r=0.

Hoffman, Patricia. Letter to Gerry Cauley, March 14, 2013. http://www.nerc.com/news/Headlines%20DL/ES-ISAC%20Letter%2014MAR13.pdf.

———. Letter to Tom Fanning and Fred Gorbet, August 5, 2014. http://www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20%28CRISP%29.pdf.

———. Plenary lecture, Resilience Week 2015 Conference, August 20, 2015, Philadelphia, PA.

Homeland Security Missions: Written Testimony Before the House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications. 114th Cong., June 10, 2015. http://www.dhs.gov/news/2015/06/10/written-testimony-fema-house-homeland-security-subcommittee-emergency-preparedness.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

ICS515: ICS Active Defense and Incident Response. Course offered by SANS Institute. https://www.sans.org/course/industrial-control-system-active-defense-and-incident-response.

IEEE Computer Society. *IEEE Guide for Information Technology—System Definition—Concept of Operations (ConOps) Document*. IEEE Standard 1362-1998. Piscataway, NJ: IEEE, March 19, 1998.

Industrial Control Systems Cyber Emergency Response Team. "Advisory: ICS-Focused Malware (ICSA-14-178-01)." Original release date July 1, 2014. https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01.

———. "Alert (ICS-ALERT-14-281-01B): Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)." Original release date December 10, 2014. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

———. *ICS-CERT Monitor*, July/August 2011 issue. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf.

———. *ICS-CERT Monitor*, May/June 2015 issue. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

Keogh, Miles, and Christina Cody. *Cybersecurity for State Regulators, with Sample Questions for Regulators to Ask Utilities*. Washington, DC: National Association of Regulatory Utility Commissioners, February 2013. http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf.

Keogh, Miles, and Sharon Thomas. *Regional Mutual Assistance Groups: A Primer*. Washington, DC: National Association of Regulatory Utility Commissioners, November 2015. http://www.slideshare.net/SharonThomas27/naruc-rmag-paper-1122015.

Macias, Victor R. "Game Changing Pivot." Master's thesis, University of Maryland Baltimore County, 2015.

Malchow, Jan-Ole, Daniel Marzin, Johannes Klick, Robert Kovacs, and Volker Roth. "PLC Guard: A Practical Defense against Attacks on Cyber-Physical Systems." In *Proceedings of the IEEE Conference on Communications and Network Security*, 326–334. Piscataway, NJ: IEEE, 2015.

Mansfield, Matthew, and William Linzey. *Hurricane Sandy Multi-State Outage & Restoration Report*. Baltimore: Maryland Public Service Commission, February 2013.

MISO. *MISO Operating Procedures*. Carmel, IN: MISO, 2015. https://www.misoenergy.org/Library/Repository/Communication%20Material/One-Pagers/One%20Pager%20-%20MISO%20Operating%20Procedures.pdf.

The Moreland Commission to Investigate Public Corruption. *Moreland Commission Report on Utility Storm Preparation and Response: Final Report*. New York: Moreland Commission, June 22, 2013. http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/MACfinalreportjune22.pdf.

National Emergency Management Association. "The EMAC Response to Hurricane Sandy." Accessed January 13, 2016. http:/www.nemaweb.org/index.php/54-em-advocate/emac-news-archive/566-the-emac-response-to-hurricane-sandy.

New York City. "Hurricane Sandy After Action Report and Recommendations to Mayor Michael R. Bloomberg." New York City, May 2013. http://www.nyc.gov/html/recovery/downloads/pdf/sandy_aar_5.2.13.pdf.

New York State Division of Military & Naval Affairs. "Hurricane Sandy After Action Review." Presentation to New York Military Forces. February 1, 2013.

North American Electric Reliability Corporation. *Cyber Attack Task Force: Final Report*. Washington, DC: North American Electric Reliability Corporation, 2012. http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf.

———. *Cyber Security Reliability Standards CIP V5 Transition Guidance: ERO Compliance and Enforcement Activities during the Transition to the CIP Version 5 Reliability Standards.* Washington, DC: North American Electric Reliability Corporation, August 12, 2014. http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf.

———. "Electricity ISAC." http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

———. *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: North American Electric Reliability Corporation, September 29, 2015. http://www.nerc.com/files/glossary_of_terms.pdf.

———. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. Washington, DC: North American Electric Reliability Corporation, 2010. http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

———. *Industry Advisory: Preventable SCADA/EMS Events – II*. Washington, DC: North American Electric Reliability Corporation. http://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/Preventable_SCADA_EMS_Events_II.pdf.

———. *NERC Operating Manual*. Washington, DC: North American Electric Reliability Corporation, August 2014. http://www.nerc.com/comm/OC/Pages/Operating-Manual.aspx.

———. Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations.* Washington, DC: North American Electric Reliability Corporation, 2012. http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

National Governors Association. *Governor's Guide to Mass Evacuation 2014*. Washington, DC: National Governors Association, 2014. http://www.nga.org/files/live/sites/NGA/files/pdf/GovGuideMassEvacuation.pdf.

NYS2100 Commission. *Recommendations to Improve the Strength and Resilience of the Empire State's Infrastructure*. New York: Office of New York City Mayor, January 11, 2013. http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS2100.pdf.

O'Neil, L. R., T. J. Vanderhorst Jr., M. J. Assante, J. Januszewski III, D. H. Tobey, R. Leo, T. J. Conway, and K. Perman. *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report*. Richland, WA: Pacific Northwest National Laboratory, July 2013. http://energy.gov/sites/prod/files/2013/12/f6/SPSP_Phase2_Summary_Final_Report.pdf.

Paletta, Damian. "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent." *Wall Street Journal*, September 8, 2015. http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541.

Panetta, Leon. "Memorandum for Secretaries of the Military Departments: Actions to Improve Defense Support in Complex Catastrophes." Secretary of Defense Memorandum, US Department of Defense, July 20, 2012.

Pellerin, Cheryl. "Rogers: Cybercom Defending Networks, Nation," *DoD News, Defense Media Activity*, August 18, 2014. http://www.defense.gov/news/newsarticle.aspx?id=122949.

Peniston, Bradley. "Work: 'The Age of Everything Is the Era of Grand Strategy.'" *Defense One*, November 2, 2015. http://www.defenseone.com/management/2015/11/work-age-everything-era-grand-strategy/123335/.

Pennsylvania Public Utility Commission *Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities*. Harrisburg, PA: Pennsylvania Public Utility Commission. http://www.puc.pa.gov/general/pdf/Cybersecurity_Best_Practices_Booklet.pdf.

Perrow, Charles. *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books, 1984.

PJM. *Fundamentals of Transmission Operations: Conservative Operations.* Audubon, PA: PJM, October 3, 2013. http://www.pjm.com/~/media/training/new-pjm-cert-exams/foto-lesson9-conservative-operations.ashx.

Reagan, B. Jim. "Mutual Assistance: Changing a Paradigm?" Talk presented at California Utilities Emergency Association Annual Meeting, San Diego, CA, June 6, 2013. www.cueainc.com/documents/Mutual%20Assistance.pptx.

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 USC.

Rogers, Michael S. *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong., September 29, 2015. http://www.armed-services.senate.gov/imo/media/doc/Rogers_09-29-15.pdf.

Samuelsohn, Darren. "Inside the NSA's Hunt for Hackers." *Politico*, December 9, 2015. http://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330.

SERC Reliability Corporation. *Guideline: Conservative Operations Guidelines*. Charlotte, NC: SERC Reliability Corporation, May 20, 2015. http://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-%2805-20-15%29.pdf?sfvrsn=2.

Shields, Raymond. "Speech to NGAUS-2013." Speech delivered at 135th NGAUS General Conference & Exhibition, Honolulu, HI, September 23, 2013.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Stacey, Brent. *United States House of Representatives Science Subcommittee on Energy and Science Subcommittee on Research and Technology*, October 21, 2015. http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf.

State of Michigan Executive Office. *Michigan Cyber Disruption Response Strategy*. Lansing, MI: State of Michigan Executive Office, September 16, 2013. https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.

Stockton, Paul. "Wrap-Up: Defense Support in Hurricane Sandy." Memorandum to the US Secretary of Defense, November 27, 2012.

Uccellini, Louis. "Sandy—One Year Later." *Weather Ready Nation*, October 28, 2013. http://www.nws.noaa.gov/com/weatherreadynation/news/131028_sandy.html#.VqvIaLEo7Gg.

US Department of Defense. *Cyber Guard 14-1: After Action Report*. Washington, DC: US Department of Defense, September 2014.

———. *The DoD Cyber Strategy*. Washington, DC: US Department of Defense, April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

———. Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, Installation Energy. *Energy Resilience Business Case Analysis Study*. Washington, DC: US Department of Defense, forthcoming.

———. "History of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs: Superstorm Sandy Response Narrative," Draft, 2013.

———. *Hurricane Sandy After Action Review OASD(HD&ASA) Staff Top Ten List: What Worked Well and Needs Improvement*. Washington, DC: US Office of the Assistant Secretary of Defense, 2012.

———. *Mission Assurance Strategy.* Washington, DC: US Department of Defense, April 2012.

———. "Talking Points for Deputy Secretary of Defense: Hurricane Sandy After Action Review." Washington, DC: US Office of the Secretary of Defense, January 10, 2013.

———. *Strategy for Homeland Defense and Defense Support of Civil Authorities*. Washington, DC: US Department of Defense, February 2013. http://fas.org/man/eprint/homedefstrat.pdf.

US Department of Energy. *The DOE Energy Response Plan*. Version 1.0. Washington, DC: US Department of Energy, February 2015.

———. *Emergency Support Function #12 – Energy Annex*. Washington, DC: US Department of Energy, January 2008. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nrf-esf-12.pdf.

———. Office of Electricity Delivery and Energy Reliability. *Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement*. Washington, DC: US Department of Energy, February 26, 2013.

———. OE-30 Energy Response Organization. Washington, DC: US Department of Energy, August 2015.

———. "SPIDERS JCTD Smart Cyber-Secure Microgrids." http://energy.gov/eere/femp/spiders-jctd-smart-cyber-secure-microgrids.

US Department of Homeland Security. *Coordinating Federal Support for Fusion Centers*. Washington, DC: US Department of Homeland Security, August 2012. http://www.dhs.gov/sites/default/files/publications/coordinating-federal-support-for-fusion-centers-flyer-compliant.pdf.

———. *Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program*. Washington, DC: US Department of Homeland Security, 2014. https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

———. *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: US Department of Homeland Security, August 5, 2013. https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf.

———. *National Cyber Incident Response Plan*. Interim version. Washington, DC: US Department of Homeland Security, September 2010. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

———. *National Preparedness Goal*. 1st ed. Washington, DC: US Department of Homeland Security, September 2011. http://www.fema.gov/pdf/prepared/npg.pdf.

———. *National Response Framework*. 2nd ed. Washington, DC: US Department of Homeland Security, May 2013. http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

US Federal Emergency Management Agency. *Hurricane Sandy FEMA After-Action Report*. Washington, DC: US Federal Emergency Management Agency, July 1, 2013. http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf.

———. "Hurricane Sandy: A Timeline." Washington, DC: US Federal Emergency Management Agency, April 24, 2013. http://www.fema.gov/media-library-data/20130726-1912-25045-8743/hurricane_sandy_timeline.pdf.

———. "National Level Exercise 2012: Cyber Capabilities Tabletop Exercise." https://www.fema.gov/media-library/assets/documents/26845.

———. *National Level Exercise 2012: Quick Look Report*. Washington, DC: Department of Homeland Security, March 2013. http://www.fema.gov/media-library-data/20130726-1911-25045-9856/national_level_exercise_2012_quick_look_report.pdf.

US Federal Energy Regulatory Commission. *Extraordinary Expenditures Necessary to Safeguard*. Docket No. PL01-6-00096 FERC ¶ 61,299. Statement of policy, 2001. http://www.iso-ne.com/committees/comm_wkgrps/trans_comm/tariff_comm/mtrls/2002/oct102002/A4_1466800.pdf.

US Government Accountability Office. *Civil Support: Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe*. GAO-13-763. Washington, DC: US Government Accountability Office, September 2013. http://www.gao.gov/assets/660/658406.pdf.

———. *Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Address Electromagnetic Threats to the Electric Grid*. Statement of Christopher P. Currie, Director, Homeland Security and Justice, Before the Committee on Homeland Security and Governmental Affairs, US Senate. Washington, DC: US Government Accountability Office, July 22, 2015. http://www.gao.gov/assets/680/671971.pdf.

US Joint Chiefs of Staff. *Interorganizational Coordination During Joint Operations*. Joint Publication 3-08. Washington, DC: US Department of Defense, June 24, 2011.

US Secretary of Defense Memorandum. "Actions to Improve Defense Support in Complex Catastrophes." July 20, 2012.

US Senate. *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors: Report of the Committee on Armed Services*. 113th Cong., 2d sess., 2015. http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

US Senate Armed Services Committee. *Advance Questions for Vice Admiral Michael S. Rogers, USN: Nominee for Commander, United States Cyber Command*. 113th Cong., March 11, 2014. http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

Walsh, David C. "Danzig: Analog Has Value in Countering Cyber Threats," *Defense Systems*, September 1, 2015. https://defensesystems.com/articles/2015/09/01/danzig-interview-cyber-defense.aspx.

Work, Robert O. *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*. 114th Cong., September 29, 2015. http://www.armed-services.senate.gov/imo/media/doc/Work_09-29-15.pdf.

Zimmerman, Rae. "Planning Restoration of Vital Infrastructure Services following Hurricane Sandy: Lessons Learned for Energy and Transportation." *Journal of Extreme Events* 1, no. 1 (August 2014): 1450004-1–1450004-38.

Abbreviations and Acronyms

APPA	American Public Power Association
APT	Advanced Persistent Threat
BES	Bulk Electric System
CEO	Chief Executive Officer
CIP	Critical Infrastructure Protection
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
EMAC	Emergency Management Assistance Compact
EMS	Energy Management System
ESCC	Electricity Subsector Coordinating Council
ESF	Emergency Support Function
ETR	Estimated Time of Restoration
FAST	Fixing America's Surface Transportation (Act)
FEMA	Federal Emergency Management Agency
HMI	Human-Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
NCIRF	National Cyber Incident Response Framework
NCIRP	National Cyber Incident Response Plan
NERC	North American Electric Reliability Corporation
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NLE	National Level Exercise
NOAA	National Oceanic and Atmospheric Administration
NRCC	National Response Coordination Center
NRE	National Response Event

NRECA	National Rural Electric Cooperative Association
NRF	*National Response Framework*
OT	Operational Technology
POIA	Power Outage Incident Annex
PUC	Public Utility Commission
RADICS	Rapid Attack Detection, Isolation and Characterization
RFA	Request for Assistance
RTO	Regional Transmission Organization
SCADA	Supervisory Control and Data Acquisition
USCYBERCOM	US Cyber Command

Acknowledgments

I thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Terry Boston (formerly with PJM); Gerry Cauley (NERC); Richard Danzig (Johns Hopkins University Applied Physics Laboratory); Daniel J. Elmore (Idaho National Laboratory); Tom Fanning (Southern Company); Dave Halla (NERC/E-ISAC); Debora Lavoy (Narrative Builders); Martin Libicki (US Naval Academy Cyber Operations Center); Colonel Timothy Lunderman (US Air Force); Steven T. Naumann (Exelon Corporation); Tim Roxey (E-ISAC Chief Operations Office); Matthew Schaffer (Johns Hopkins University Applied Physics Laboratory); Brent J. Stacey (Idaho National Laboratory); Mike Wallace (formerly with Constellation Energy); and Tad White (National Security Agency). I also thank the many additional 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 the Johns Hopkins University Applied Physics Laboratory. 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 to FEMA and DHS during Superstorm Sandy, Hurricane Irene, and other disasters. Dr. Stockton also served as DOD's 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.

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 and associate provost of the Naval Postgraduate School (NPS). 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 lead co-author of "Curbing the Market for Cyberweapons" (*Yale Law & Policy Review*, 2013) and numerous other studies.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY