Blackout: A Case Study of the 2003 North American Power Outage with Exercises

Instructor Materials and Case Conclusion

Table of Contents

Blackout: A Case Study of the 2003 North American Power Outage

Instructor Materials

The 2003 North American Blackout was a widespread incident that serves as a robust case study of the Energy Sector, illustrating the unique characteristics of the Electricity Subsector and the effects of cascading failures and interdependencies for critical infrastructure security and resilience (CISR) professionals. Given the importance of planning activities for CISR professionals, the exercises center on strategy and planning activities in an interdependency-rich environment.

The goal of the case is to help learners develop proficiency in DHS/IP Core Competencies and to reinforce the learning objectives found in the Introduction to Critical Infrastructure Security and Resilience course. The case *narrative* emphasizes learning objectives found in the course lessons on Risk Analysis, Interdependencies, Regulatory Approaches, Cybersecurity, Resilience, and Preparing for the Future Risk Environment.

The case *exercises* are designed to build core competencies in Risk Analysis, Protection Measures and Mitigation Strategies, and Information Sharing through a series of exercises that target thorough and creative scenario generation and analysis. In addition, the exercises model individual and group techniques that develop divergent and convergent critical thinking skills and are designed as repeatable, practical methods those learners can apply not only in the course but also in the workplace. Exercise 1 puts learners in the shoes of a planner who is tasked with anticipating the full range of issues that will affect future resilience of the Electricity Subsector. It asks learners to enumerate the main drivers of future subsector resilience. Exercise 2 builds on exercise 1 by challenging learners to use the drivers to think thoroughly and creatively about future outcomes (scenarios). It asks students to create most likely, least likely, nightmare, and wildcard scenarios. Exercise 3 builds on exercise 2 by asking learners to analyze and create mitigation strategies for these scenarios using a Strengths-Weakness-Opportunities-Threats analysis.

The goal of the exercises is to employ sound critical thinking about strategy and planning activities, not simply to model the known outcome. As such, the exercises help the learner employ a robust and structured approach to these activities and explicitly identify the value added by using them. Many times, the value of a technique lies in the conversation that it prompts about evidence, factors, assumptions, and gaps that would otherwise be overlooked. Learners should judge their performance, therefore, on *how* they have conducted their analyses rather than on the specific case outcome.

Exercise 1. Strategic Planning Divergent Thinking Phase: Elements of Future Resilience for the Electricity Subsector.

Brainstorming is a process that follows specific rules and procedures designed to generate new ideas and concepts. The stimulus for creativity comes from two or more people bouncing ideas off each other. A brainstorming session usually exposes participants to a greater range of ideas and perspectives than any one person could generate alone, and this broadening of views typically results in a better product.

Structured Brainstorming is a systematic twelve-step process (described below) for conducting group brainstorming. It is most often used to identify key drivers or all the forces and factors that may come into play in a given situation. If, however, a group is not possible, there is still value in thinking as imaginatively and divergently as possible by adjusting the technique for use by one person. The goal of brainstorming, whether used in a group or by oneself, is to think as exhaustively as possible.

Task: What are the drivers (factors, actors, issues) that affect Electricity Subsector resilience?

Structured Brainstorming Technique Steps

Step 1: Gather a group of CISR learners.

Step 2: Pass out sticky notes and Sharpie-type pens or markers to all participants. Inform the team that there is no talking during the sticky-notes portion of the brainstorming exercise.

Step 3: Present the team with the following question: What are the drivers (factors, actors, issues) that affect Electricity Subsector resilience?

Step 4: Ask the group to write down responses to the question with a few key words that will fit on a sticky note. After a response is written down, the participant gives it to the facilitator who then reads it aloud. Sharpie-type or felt-tip pens are used so that people can easily see what is written on the sticky notes later in the exercise.

Step 5: Place all the sticky notes on a wall randomly as they are called out. Treat all ideas the same. Encourage participants to build on one another's ideas. The random placement of the sticky notes gives all ideas equal weight:

Step 6: Usually an initial spurt of ideas is followed by pauses as participants contemplate the question. After five or ten minutes there is often a long pause of a minute or so. This slowing down suggests that the group has "emptied the barrel of the obvious" and is now on the verge of coming up with some fresh insights and ideas. Do not talk during this pause even if the silence is uncomfortable.

Step 7: After two or three long pauses, conclude this divergent-thinking phase of the brainstorming session.

Step 8: Ask all participants (or a small group) to go up to the wall and rearrange the sticky notes by affinity groups (groups that have some common characteristics). Some sticky notes may be moved several times, and some may be copied if the idea applies to more than one affinity group. An example of an affinity cluster for Physical Assets follows:

Step 9: When all sticky notes have been arranged, ask the group to select a word or phrase that best describes each grouping.

Step10: Look for sticky notes that do not fit neatly into any of the groups. Consider whether such an outlier is helpful or the germ of an idea that deserves further attention.

Step 11: Assess what the group has accomplished. Can you identify key factors or forces that are particularly salient to Electricity Subsector resilience?

- Manmade Threats
- Natural Threats
- Physical Aspects of the Grid
- Human Aspects of the Grid
- Cyber Aspects of the Grid
- Legal and Regulatory Frameworks
- Financial Resources
- Industry Interests
- Communication/Information Sharing

- Scientific Advances

Analytic Value Added

Which drivers have near-term, mid-term, and longer-term consequences for Electricity Subsector resilience? Did our ideas group themselves into coherent affinity groups? Were there any outliers or sticky notes that seemed to belong in a group all by themselves? Did the outliers spark new lines of inquiry? Did the labels we generated for each group accurately capture the essence of that set of sticky notes? What additional information should we track down about the threats and vulnerabilities we generated? Where does that information reside and to whom should we speak about it?

Learners should discuss each of these questions as they group their ideas into affinity clusters and name the cluster for maximum impact. Warn students that large groups of sticky notes should signal opportunities to break up and reorganize the clusters. Usually, large groups of sticky notes are indicative of conflated ideas or groups of ideas.

Exercise 2. Strategic Planning Convergent Thinking Phase: Creating a Forward-looking Strategy

There are many factors that could shape the future of the highly interdependent Electricity Subsector. Using a scenarios technique can be a useful way to develop an understanding of the multiple ways in which a situation might evolve. The analytic value added by using scenarios techniques lies not in the specifics of the scenarios themselves but in the analytic discussion about which drivers will affect a particular scenario, the implications of each scenario for planning, and the specific action items that emerge.

Task: Using various combinations of drivers developed in Exercise 1, create a range of future scenarios for the Electricity Subsector over the next ten years.

Futures Technique Steps

Step 1: Clearly define the focal issue and the specific goals of the Simple Scenarios exercise.

Step 2: Using the affinity group drivers developed in Exercise 1, create a matrix with the list of drivers down the left side, as shown in the Table below.

Step 3: List four different scenarios—best case, worst case, and at least one other, for example, a nightmare scenario—across the top of the matrix.

	Best Case	Worst Case	Nightmare
Manmade Threats	o	--	--
Natural Threats	o	--	--
Physical Assets	+	--	--
Human Assets	+	--	--
Cyber Assets	+	--	--
Financial Resources	+	--	--
Legal and Regulatory Framework	+	--	--
Industry Interests	+	--	--

Communication	+	--	--
Scientific Advances	+	--	--

Step 4: Working across the matrix, consider how each driver would affect each scenario. Each scenario is assigned a positive, negative, or neutral value for each driver. The values are strong or positive (+), weak or negative (–), and blank if neutral or no change. ***An easy way to code the matrix is to assume that the scenario already occurred and ask, "Did driver A exert a strong, weak, or neutral influence on the outcome?"***

Step 5: Look across the matrix to evaluate how each driver discriminates among the scenarios. If a driver has the same value across all scenarios, it is not discriminating and should be deleted or further defined.

Step 6: For each scenario, use the coded matrix to illustrate how the interplay of the drivers would emerge to create the scenario. Write a no longer than one-paragraph story to describe the future scenario and/or how it might come about. In this case, for example, short future scenarios might include:

Collabora-Town: Proactively Collaborating to Increase Resilience and Accountability

In this best-case scenario, manmade threats such as terrorism do not adversely affect the resilience of the electricity subsector and natural threats are mitigated by improvements in physical, cyber, and human grid assets. Existing public-private partnerships operate cohesively, increase information sharing and provide resources that bolster education and training and allow for implementation of new smart grid technology. Government and industry resources are targeted on updating and securing cyber and physical assets and ensuring that scientific advances and emerging technologies help to harden the grid. By doing so, cyber security standards are clarified and adopted, SCADA systems are secured, and redundancies are put in place. Industry successfully implements new regulatory structures and new protocols are developed for the integration of alternative energy sources. This diversification creates redundancies in the grid and improves resilience.

Unrelia-Ville: Passivity Leads To an Insecure Grid

In this worst-case scenario, stakeholders are unable to prevent losses of physical, cyber, and human assets from manmade or natural threats, resulting in Nation-wide imbalances between supply and demand. Rolling brownouts ensue during the summer months throughout the country. This creates financial losses for U.S. industry. Financial resources are not available to support scientific advances that could

mitigate these losses. Legal and regulatory frameworks that are counter to industry interests mean that standards are not implemented or slow-rolled, leaving vulnerabilities to the grid. As a result, public confidence plummets and tensions erupt between private industry and government. This tensions lead to a break down in information sharing and a panic ensues when minor blackouts occur over the summer months. Lack of transparency and relationship building among stakeholders compound problems with communication, and implementation of industry-wide training and smart grid improvements.

Chaotica: Compounding Natural and Manmade Events
A high-magnitude earthquake on the West Coast takes down a large swath of the West Coast, particularly southern California. With the lights out for several days during the hot summer months, and social services down, looters take to the street in Los Angeles damaging property, rioting, and setting fire to local businesses. While attention turned to social unrest sparked by the earthquake, opportunistic Chinese hackers attack East Coast financial and government servers. The Dow plummets and we are at cyber war. In the face of widespread attacks on our energy infrastructure, the President urges select utilities under the most strain from cyber attacks to voluntarily shut down while the Federal Government helps to protect them from attack. Simultaneously, the Washington, D.C. metropolitan area suffers multiple failures in which one million customers lose power for a week while utilities try to discern the cause. In addition to the expense to the region, the outage causes traffic jams, water rationing, lack of sanitation, an increase in crime, and heat-related deaths among the very young and very old.

Step 7: For each scenario, describe the implications for the Electricity Subsector. The implications should be focused on variables that the CISR planners and policymakers could influence to shape the outcome.

- Collabora-Town. In this scenario, the Electricity Subsector benefits from public-private partnerships that effectively focus resources on areas like securing physical and cyber security and integrating alternative energy sources.
- Unrelia-Ville. The kind of longer-term degradation of reliability has very real impacts on public confidence, making the atmosphere ripe for social unrest when a relatively short-term event occurs. The psychological impact of these kinds of brownouts on public confidence cannot be underestimated. Media strategies should be considered in the event that brownouts of this type increase in frequency.
- Chaotica. There are low-probability, high-impact scenarios in which simultaneous events could exponentially increase the scope and duration of an outage. While these rare events are

unlikely, the scenario underscores the need to develop redundancies and information sharing mechanisms that could be relied upon should this type of situation occur.

Analytic Value Added

Which aspects of the scenarios most deserve of attention and why? Is there a particular scenario that stands out, and why? What action items emerge?

In their responses, learners should focus on both the strategic and tactical "so what" that can be derived from the process. In the notional solution above, the broader lesson is that while none of these scenarios is likely to unfold as we have described them, any number of aspects of the scenarios could occur. As a result, the scenarios should prompt thinking about similarities and differences among scenarios. Information sharing, for example, figures prominently, albeit in different ways, in each scenario. This could prompt a discussion of all of the elements of information sharing that should be considered. Action items can then emerge from this discussion; for example, any information sharing strategy must include the full range of stakeholders, from the utility customer, to the ISOs, to government agencies. The goal of this process for learners is to emphasize the full range of actors and issues that will affect electricity subsector resilience in the future and the host of issues with which planners must grapple.

Exercise 3. Strategic Planning: Strategic Planning Troubleshooting and Mitigation Strategies

Strengths-Weaknesses-Opportunities-Threats (SWOT) Analysis can be used to evaluate a future scenario by providing a framework for organizing and collecting data for strategic planning. SWOT is designed to illuminate areas for further exploration and more detailed planning, and therefore it is typically an early step in a robust policy process. SWOT analysis can also be an important part of troubleshooting plans and identifying specific actions that may improve the chances of success.

Task: Choose at least one of the future scenarios generated in Exercise 2 and enumerate the strengths, weaknesses, opportunities, and threats for the scenario.

SWOT Technique Steps

Step 1: Clearly define the future scenario to be analyzed. Use the paragraph generated in Exercise 2 as a point of departure.

Step 2: Enumerate each of the Strengths Weaknesses, Opportunities, and Threats associated with the future scenario.

Step 3: Use the SWOT table to generate as many strengths, weaknesses, opportunities, and threats as possible. If there are none, use the drivers generated in Exercise 1 to prompt deeper thinking about the scenario. Also, challenge any underlying assumptions about those already developed to generate even more ideas.

In the example below, participants used the Unrelia-Ville scenario generated in Exercise 2. As a result, the SWOT analysis reflects the reality described in the scenario. Using the scenario as the basis for the analysis can draw out new and interesting elements and challenge assumptions.

Strengths	**Weaknesses**
1. Legal and Regulatory Frameworks now exist. 2. Taskforce recommendations have been implemented, albeit unevenly.	1. Information sharing is spotty. 2. Financial resources not allocated effectively. 3. Physical infrastructure is ageing. 4. Legal and Regulatory Frameworks in place but are not fully implemented.
Opportunities	**Threats**
1. Repeated brownouts create atmosphere in which industry and public is ready for change. 2. Review and update emergency plans and communication. 3. Brownouts make problem areas more visible. 4. Current situation can be used to catalyze Industry/Scientific Community/ Government cooperation.	1. Cyber threat is looming and may compound vulnerabilities of aging infrastructure. 2. Supply does not meet demand. 3. Lack of innovation leaves us flat footed.

Analytic Value Added:

Using the results of the SWOT analysis, numerate how can one might bolster and use strengths, mitigate and improve upon weaknesses, create and exploit opportunities, and counter threats? Do any ideas emerge that deserve immediate attention or action, and why?

The SWOT analysis may be used for one or all of the scenarios generated. In every case, the most important aspect of the SWOT is the detailed and action-oriented conversation that it prompts about the scenario. Rather than simply stopping at strengths and weaknesses, it prompts learners to think more deeply about hitherto hidden opportunities and threats that could be exploited and countered. In this case, for example, the legal and regulatory structures put in place could be both strengths and weaknesses if overlooked or not fully implemented. When considered from the standpoint of opportunity creation, however, the situation looks different. For example, opportunities may rest in the realm of legal and regulatory frameworks, particularly if standards are promulgated in a cooperative spirit. In this regard, developing stronger partnerships stands out as a key element for future success.

Case Conclusion

The Northeast Blackout of 2003 only lasted forty hours, but its effect on efforts to improve electricity subsector resilience is still being felt. Since 2003, the Federal Government and industry have taken a number of steps to meet the challenges posed by the blackout, specifically with an eye toward enhancing the legal, regulatory, information sharing, and technological aspects of resilience that it highlighted.

A central issue following the Blackout was the voluntary nature of North American Electric Reliability Corporation (NERC) standards. The Energy Policy Act of 2005 addressed this issue by not only authorizing the creation of an electric reliability organization (ERO) for North America, but also making utility compliance mandatory.[1] Moreover, it expanded the role of the Federal Energy Regulatory Commission (FERC) by requiring it to solicit, enforce, and approve the new reliability standards from NERC.[2] In 2006 FERC certified NERC as the national ERO, and in 2007 NERC reliability standards became mandatory and enforceable in the United States. By 2008, just one year later, FERC had approved 96 new reliability standards covering issues relating to all aspects of reliability, including training, vegetation maintenance, voltage, and communication and information sharing, among others.[3]

In addition to these legal and regulatory enhancements, new presidential directives were put in place to improve information sharing for all critical infrastructure sectors as well as physical and cyber grid security. Under the auspices of Homeland Security Presidential Directive-7 (HSPD-7) signed in December 2003, the United States Department of Energy (DOE) serves as the Energy Sector Specific Agency (SSA), a role that requires close collaboration with government agencies—via the Government Coordinating Council (GCC) established in 2004—and private industry—via the Electricity Sector Coordinating Council (SCC) and Petroleum and Natural Gas SCC.[4] By 2010, the Departments of Energy and Homeland Security, in coordination with the GCC and SCCs, made information sharing and communication; physical and cyber security; coordination and planning; and building public confidence the chief goals cited in the Energy Sector-Specific plan Annex to the National Infrastructure Protection Plan. In 2011, Presidential Policy Directive-8 (PPD) on National Preparedness was promulgated to "strengthen the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters."[5] In 2013, the Presidential Policy Directive-21 (PPD) on Critical Infrastructure Security and Resilience updated HSPD-7 "to adjust to the new risk environment, key lessons learned, and drive toward enhanced capabilities." The PPD-21 cited the need "to leverage and integrate successes in [physical and cyber security]" and specifically to:

- Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
- Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
- Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.[6]

In the decade following the Blackout, new smart grid technologies have been developed and are improving the industry's ability to monitor, control, and share information about the grid. These smart grid technologies use two-way computer-based communication technology to automate certain aspects of real-time monitoring and system controls—automation that was lacking during the 2003 Blackout.[7] Federal support for technological advancements in grid SCADA systems in particular has paved the way for significant improvements. In 2007, Title XIII of the Energy Independence and Security Act (EISA) established a range of Department of Energy-led groups and initiatives to support development of an interoperable Smart Grid. The smart aspects of these new technologies range from new "smart" meters that can be used to improve energy efficiency, to systems that allow for better integration of renewable energy sources and customer participation in resilience, to highly sophisticated sensors that monitor generator capacity.[8] While adoption of smart grid technology is not yet universal, it is increasingly employed throughout the United States.[9] A National Science and Technology Council progress report published in 2013 indicated that 10.8 million smart electric meters had been installed since early 2009, with at least 15.5 million installed meters expected by 2015. These smart meters provide real-time data about when and how much energy is being consumed to utilities and consumers about energy use. This not only encourages consumer conservation but also helps utilities to locate remotely the source of outages and restore power through the Internet when outages occur.[10]

Despite these improvements, the future continues to hold many potential challenges arising from both manmade and natural threats. In 2010, for example, NERC issued a joint assessment with the Department of Energy about threats to the electricity subsector from high-impact, low-frequency (HILF) events. Although rare, these events included coordinated cyber, physical, and blended attacks, as well as major natural disasters such as earthquakes, hurricanes, pandemics, and geomagnetic disturbances. In addition to identifying these latent threats, the report included stakeholder "proposals for action" corresponding to each event type.[11] Furthermore, according to a 2012 US Government Accountability Office report on the challenges to securing the electric grid, some of these hitherto low-frequency events, such as coordinated cyber attacks, are becoming more frequent.[12] NERC and the industry established four task forces to address the highest-priority HILF risks and released their reports during 2011 and 2012.

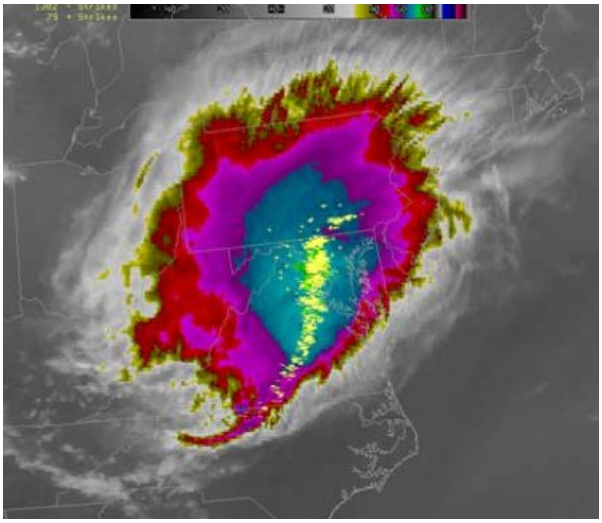
Indeed, the cyber threat looms large as the industry transitions to the smart grid. The Director of National Intelligence in 2011 noted a "dramatic increase in cyber activities targeting US computers and systems, including a more than tripling of malicious software."[13] During a 2012 House Energy and Commerce Subcommittee hearing the GAO Director of Information Security Issues highlighted both the potential upsides and downsides to technological advancements in the electric grid saying:

> "The electricity industry is in the midst of a major transformation as a result of smart grid initiatives and this has led to significant investments by many entities, including utilities, private companies, and the federal government. While these initiatives hold the promise of significant benefits, including a more resilient electric grid, lower energy costs, and the ability to tap into alternative sources of

power, the prevalence of cyber threats aimed at the nation's critical infrastructure and the cyber vulnerabilities arising from the use of new technologies highlight the importance of securing smart grid systems."[14]

Even if these cyber-related challenges are met, natural threats such as weather-related events like the 2012 Derecho or Superstorm Sandy illustrate how quickly an event can have a massive impact on electric power supply. In the case of the June 2012 Derecho that struck a swath of the Midwest and Mid-Atlantic regions, event onset was sudden and recovery was prolonged by the lack of communication in some cases that was caused by primary and secondary power source failures, according to a report by the Federal Communications Commission.[15] In some cases, smart grid technology may have reduced, if not completely mitigated the impact of the storm: the National Science and Technology Council report released in 2013 also noted that a Tennessee utility concluded that smart grid investments cut its outages in half during the derecho.[16] In the case of Superstorm Sandy, an unlikely hurricane track into the New Jersey shore came to fruition, leveling houses and lower Manhattan in the dark for a week and leveling structures along the New Jersey shoreline.

Figure 1: A Satellite Image of the 2012 Derecho



Source: National Weather Service, http://www.erh.noaa.gov/lwx/events/svrwx_20120629/.

These low-probability, high-impact scenarios are the types of events for which planners must prepare although the chances of experiencing one, much less two, such events in one year is very low. In every case, however, the electricity subsector plays a critical role in how quickly affected areas can respond to and recover from the event. Careful planning and imaginative solutions to these types of challenges must figure prominently if critical infrastructure protection professionals are to improve the resilience of the electricity subsector for the future.

Key Takeaways

Active consideration of the full range of factors that can drive future outcomes is essential to developing carefully considered strategies and plans to address them. To do so requires an open mind and a diverse group of thinkers who have resilience as their common goal. Using techniques such as those found in the previous exercises to prompt thorough and creative thinking about factors that will shape future outcomes can spark conversations about otherwise un-explicated forces and factors and guide group thinking in productive directions.

[1] In 1997 an Electric System Reliability Task Force established by the Department of Energy, and an independent Electric Reliability Panel ("Blue Ribbon" panel) formed by NERC determined that grid reliability rules must be mandatory and enforceable. Both groups recommended the creation of an independent, audited self-regulatory electric reliability organization.

[2] JR Minkel, "The 2003 Northeast Blackout—Five Years Later," *Scientific American*, August 13, 2008, www.scientificamerican.com

[3] NERC Webpage, Reliability Standards, 2013, http://www.nerc.com/page.php?cid=2%7C20.

[4] HSPD-7, Department of Homeland Security, http://www.dhs.gov/homeland-security-presidential-directive-7.

[5] Presidential Policy Directive PPD-8: National Preparedness, March 30, 2011, http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

[6] "Fact Sheet: Presidential Policy Directive on Critical Infrastructure Security and Resilience, The White House," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/fact-sheet-presidential-policy-directive-critical-infrastructure-securit.

[7] Smart Grid, U.S. Department of Energy, http://energy.gov/oe/technology-development/smart-grid.

[8] Smart Grid, U.S. Department of Energy, http://energy.gov/oe/technology-development/smart-grid.

[9] The Smart Grid: An Introduction, Prepared for the U.S. Department of Energy by Litos Strategic Communication, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf.

[10] Zack Colman "White House Official: Power Grid Updates Needed to Mitigate Extreme Weather," The Hill, February 26, 2013, thehill.com.

[11] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," NERC and the U.S. Department of Energy, June 2010, http://www.nerc.com/files/HILF.pdf.

[12] Press Release: Committee Examines Smart Grid Technologies as Part of Ongoing Effort to Improve Cybersecurity, United States House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, February 28, 2012, http://energycommerce.house.gov/press-release/committee-examines-smart-grid-technologies-part-ongoing-effort-improve-cybersecurity.

[13] Challenges in Security the Electric Grid, US GAO, http://www.gao.gov/assets/600/592508.pdf.

[14] Press Release: Committee Examines Smart Grid Technologies as Part of Ongoing Effort to Improve Cybersecurity, United States House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, February 28, 2012, http://energycommerce.house.gov/press-release/committee-examines-smart-grid-technologies-part-ongoing-effort-improve-cybersecurity.

[15] Derecho Report and Recommendations, Federal Communications Commission, January 10, 2013, http://www.fcc.gov/document/derecho-report-and-recommendations.

[16] Zack Colman "White House Official: Power Grid Updates Needed to Mitigate Extreme Weather," The Hill, February 26, 2013, thehill.com.