





The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop

ISBN
978-0-309-29395-2

42 pages
8.5 x 11
PAPERBACK (2013)

David W. Cooke, Rapporteur; Planning Committee for the Workshop on the Resilience of the Electric Power System to Terrorism and Natural Disasters; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Research Council

 Add book to cart

 Find similar titles

 Share this PDF



Visit the National Academies Press online and register for...

- ✓ Instant access to free PDF downloads of titles from the
 - NATIONAL ACADEMY OF SCIENCES
 - NATIONAL ACADEMY OF ENGINEERING
 - INSTITUTE OF MEDICINE
 - NATIONAL RESEARCH COUNCIL
- ✓ 10% off print titles
- ✓ Custom notification of new releases in your field of interest
- ✓ Special offers and discounts

Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences. Request reprint permission for this book

The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters

SUMMARY OF A WORKSHOP

David W. Cooke, *Rapporteur*

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

Support for this project was provided by BP America, GE Energy, General Motors Corporation, and Intel Corporation. Support was also provided by the National Academy of Sciences through the following endowed funds created to perpetually support the work of the National Research Council: Thomas Lincoln Casey Fund, Arthur L. Day Fund, W.K. Kellogg Foundation Fund, George and Cynthia Mitchell Endowment for Sustainability Science, and the Frank Press Fund for Dissemination and Outreach. Any opinions, findings, or conclusions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations that provided support for the project.

International Standard Book Number-13: 978-0-309-29395-2

International Standard Book Number-10: 0-309-29395-2

Copies of this report are available in limited supply, free of charge, from: Board on Energy and Environmental Systems, National Research Council, 500 Fifth Street, NW, Keck W934, Washington, DC 20001, (202) 334-3344.

Additional copies of this report are available for sale from: The National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001, (800) 624-6242 or (202) 334-3313, <http://www.nap.edu>.

Copyright 2013 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America.

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. C. D. Mote, Jr., is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. C. D. Mote, Jr., are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

PLANNING COMMITTEE FOR THE WORKSHOP ON THE RESILIENCE OF THE ELECTRIC POWER SYSTEM TO TERRORISM AND NATURAL DISASTERS

M. GRANGER MORGAN, NAS,¹ Carnegie Mellon University, *Chair*

CLARK W. GELLINGS, Electric Power Research Institute

DAVID K. OWENS, Edison Electric Institute

LOUIS L. RANA, Consolidated Edison Company (retired)

RICHARD E. SCHULER, Cornell University

SUSAN F. TIERNEY, Analysis Group

Staff

PETER BLAIR, Executive Director, Division on Engineering and Physical Sciences

DAVID W. COOKE, Associate Program Officer

ALAN CRANE, Senior Scientist

JAMES J. ZUCCHETTO, Director, Board of Energy and Environmental Systems

¹ National Academy of Sciences.

BOARD ON ENERGY AND ENVIRONMENTAL SYSTEMS

ANDREW BROWN, JR., NAE,¹ Delphi Corporation, Troy, Michigan, *Chair*
WILLIAM F. BANHOLZER, NAE, Dow Chemical Company, Midland, Michigan
WILLIAM CAVANAUGH III, NAE, Progress Energy (retired), Raleigh, North Carolina
PAUL A. DeCOTIS, Long Island Power Authority, Albany, New York
CHRISTINE EHLIG-ECONOMIDES, NAE, Texas A&M University, College Station
SHERRI GOODMAN, CNA, Alexandria, Virginia
NARAIN G. HINGORANI, NAE, Independent Consultant, San Mateo, California
ROBERT HUGGETT, Independent Consultant, Seaford, Virginia
DEBBIE NIEMEIER, University of California, Davis
DANIEL NOCERA, NAS,² Massachusetts Institute of Technology, Cambridge
MARGO OGE, Environmental Protection Agency (retired), McLean, Virginia
MICHAEL OPPENHEIMER, Princeton University, Princeton, New Jersey
JACKALYNE PFANNENSTIEL, Independent Consultant, Piedmont, California
DAN REICHER, Stanford University, Stanford, California
BERNARD ROBERTSON, NAE, Daimler-Chrysler (retired), Bloomfield Hills, Michigan
GARY ROGERS, FEV, Inc., Auburn Hills, Michigan
ALISON SILVERSTEIN, Consultant, Pflugerville, Texas
MARK THIEMENS, NAS, University of California, San Diego
RICHARD WHITE, Oppenheimer & Company, New York City
ADRIAN ZACCARIA, NAE, Bechtel Group (retired), Frederick, Maryland

Staff

JAMES J. ZUCCHETTO, Senior Board/Program Director
DANA CAINES, Financial Associate
DAVID W. COOKE, Associate Program Officer
ALAN CRANE, Senior Scientist
K. JOHN HOLMES, Senior Program Officer/Associate Director
LaNITA JONES, Administrative Coordinator
ALICE V. WILLIAMS, Senior Program Assistant
JONATHAN YANGER, Senior Project Assistant

¹ National Academy of Engineering.

² National Academy of Sciences.

Preface

The National Research Council (NRC) released a report, *Terrorism and the Electric Power Delivery System*,¹ in 2012 that analyzed the vulnerability of the electric grid to terrorist attacks and measures to reduce that vulnerability. The report had been written in 2007 for the Department of Homeland Security (DHS), but publication was delayed because of security concerns. While most of the committee's findings were still relevant, many developments affecting vulnerability had occurred in the interval. In order to expand familiarity with the report among potential users and explore recent and future trends, a workshop was held on February 27-28, 2013. The specific goals of the workshop were to discuss the committee's results, what had changed in recent years, and how lessons learned about the grid's resilience to terrorism could be applied to other threats to the grid resulting from natural disasters. The workshop focused on five key areas: physical vulnerabilities of the grid; cybersecurity; mitigation and response to outages; community resilience and the provision of critical services; and future technologies and policies that could enhance the resilience of the electric power delivery system.

This report is a summary of the presentations and discussions at the workshop. No effort was made to achieve any consensus views of the participants or the planning committee. The summary does not contain any conclusions or recommendations on the part of the NRC or any advice to the government. Nor does it represent a viewpoint of the National Academies or any of its constituent units, and no priorities are implied by the order in which the issues are presented. The workshop was recorded, and the videos may be viewed at http://sites.nationalacademies.org/DEPS/BEES/DEPS_081103.

The workshop was made possible through the hard work and dedication of the individuals who served on the NRC Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack (Appendix A) as well as the invited presenters and workshop participants listed in Appendix B.

Special recognition is due to Daniel Ribas at Spark Street Lighting, who provided an excellent webcast of the workshop that was invaluable in the writing of this summary, and Sheryl Bottner of the NRC's Division on Engineering and Physical Sciences (DEPS), who facilitated putting online both the presentations from the workshop and the webcast.

The committee is grateful to Peter Blair, DEPS Executive Director, and Paul Michaels of the NRC's Office of Security for their work with the Department of Homeland Security to release an unclassified version of the report *Terrorism and the Electric Power Delivery System*.

This workshop summary has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the

¹ National Research Council, 2012, *Terrorism and the Electric Power Delivery System*, The National Academies Press, Washington, D.C..

NRC's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for quality and objectivity. The review comments and draft manuscript remain confidential to protect the integrity of the review process. The author would like to thank the following individuals for their review of this report:

Anjan Bose, Washington State University,
Paul A. DeCotis, Long Island Power Authority,
Narain G. Hingorani, Independent Consultant,
Paul J. Kern, The Cohen Group,
Richard E. Schuler, Cornell University,
Alison Silverstein, Independent Consultant, and
Bruce F. Wollenberg, University of Minnesota.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the content of the report, nor did they see the final draft of the report before its release. The review of this report was overseen by Chris Whipple of Environ. Appointed by the NRC, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the author and the institution.

David W. Cooke
Rapporteur

Contents

1	INTRODUCTION	1
	Origin of the Workshop, 1	
	A Changing Climate, 2	
2	GRID INFRASTRUCTURE	4
	Attacking the Infrastructure, 5	
	Natural Disasters, 6	
	Solutions, 7	
3	CYBERSECURITY OF THE GRID	10
	Merging of Infrastructures, 10	
	Risk Assessment and Cybersecurity, 12	
	Solutions, 13	
4	RESPONDING TO OUTAGES	15
	Restoration of Power, 15	
	Critical Services and Community Resilience, 16	
	Solutions, 18	
5	THE FUTURE OF THE GRID	22
	Distributed Generation, 22	
	The Smart Grid, 23	
6	SUMMARY OF MAIN POINTS RAISED IN WORKSHOP DISCUSSIONS	25
APPENDIXES		
A	Authorship of <i>Terrorism and the Electric Power Delivery System</i>	27
B	Workshop Participants	28
C	Workshop Presentations and Discussions	30

1

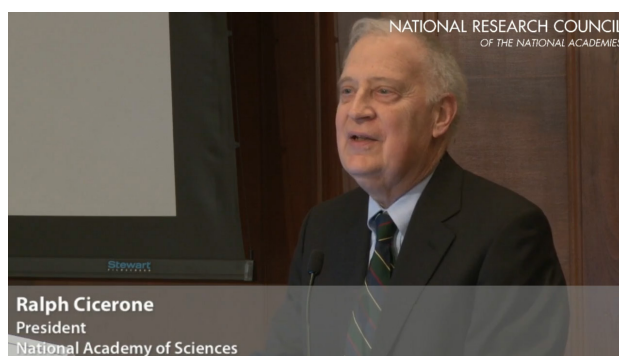
Introduction

The electric power transmission and distribution system (“the grid”¹) is an extraordinarily complex network of wires, transformers, and associated equipment and control software designed to transmit electricity from where it is generated, usually in centralized power plants, to commercial, residential, and industrial users. Because the U.S. infrastructure has become increasingly dependent on electricity, vulnerabilities in the grid have the potential to cascade well beyond whether the lights turn on, impacting among other basic services such as the fueling infrastructure, the economic system, and emergency services.

Origin of the Workshop

In 2007, the National Research Council (NRC) prepared a report responding to a request from the Department of Homeland Security (DHS) to examine the vulnerability of the grid to terrorist attack. However, the report was classified out of concern that it might help terrorists target the electric grid. In 2012, the NRC was able to work with the DHS to release an unclassified report, *Terrorism and the Electric Power Delivery System*,² in November 2012, just 2 weeks after Hurricane Sandy impacted the northeastern United States with flooding and power outages.

Given the amount of time that had passed since completion of the report in 2007 and its eventual release in 2012, the NRC and the committee wanted to ascertain whether much had changed during this 5-year period and to identify possible efforts going forward. Because of the shifting context for the vulnerability of the electric power system, the focus of the workshop was also broadened to include impacts from natural disasters as well



as intelligent agents. Thus, the NRC and the committee responsible for writing the 2007 report held a workshop on the resilience of the electric power delivery system in response to terrorism and natural disasters. The purpose was not to translate the entire report into the present, but to

¹ It should be noted that although the grid tends to be referred to as a single unit, in fact it is comprised of three separate grids with few connections between them: the Eastern Interconnection, the Western Interconnection, and the Texas Interconnection.

² National Research Council, 2012, *Terrorism and the Electric Power Delivery System*, The National Academies Press, Washington, D.C.

focus on key issues relevant to making the grid sufficiently robust that it could handle inevitable failures without disastrous impact.

The workshop took place at the National Academy of Sciences on February 27-28, 2013, as part of the dissemination of the committee's work. **Ralph Cicerone, President of the National Academy of Sciences**, noted at the start of the workshop that new needs and desires are developing in electrical power distribution, and that it is the responsibility of the NRC to ensure that the work of the committee is as timely and relevant as possible, despite the delayed public release of its report. Building on the committee's report, the workshop focused on physical vulnerabilities and the cybersecurity of the grid as well as ways in which communities respond to widespread outages and how to minimize these impacts. Finally, the workshop also touched on the grid of tomorrow and how resilience can be encouraged and built into the grid in the future.

A Changing Climate

Granger Morgan, Carnegie Mellon University (CMU), chair of the committee that authored *Terrorism and the Electric Power Delivery System*,³ noted at the outset of the workshop that although that report may have focused on "attacks," 80 to 90 percent of the discussion in the report is relevant to vulnerabilities beyond terrorism. Given the increasing probability that severe weather events are occurring owing to climate change, there was a great amount of discussion on how to begin to assess the vulnerabilities to these nonterrorist events moving forward.

David Kaufman, Federal Emergency Management Agency (FEMA), noted that planning tends to assume current capacity and further assumes that events in the future will be similar to ones in the past. While this is a useful starting point, it is crucial to understand outcomes that can break the system. As 100-year floods become 50- or even 20-year floods, how should adjustments be made? According to Mr. Kaufman, even if one is able to acknowledge the risk, it is difficult to determine how to address it and who will be responsible for the costs.

Gerald Galloway, University of Maryland, noted that insurance agencies are beginning to recognize that catastrophic occurrences are becoming increasingly frequent as global climate change continues to alter weather patterns, and they are starting to factor this into their risk assessment models. While Hurricane Sandy may have been the most recent natural disaster to broadly impact national infrastructure, he also pointed to the tsunami in Japan that led the Fukushima Dai-ichi nuclear disaster in 2012 and the impact of Hurricanes Rita and Katrina on the Gulf Coast in 2005 as catastrophic events that have led to major upheaval. In 2011 alone, Dr. Galloway noted, \$55 billion in economic damage was due to weather events in the United States, with 14 events causing more than \$1 billion in damage each. He said that no person or place is immune to these events.

³ National Research Council, 2012, *Terrorism and the Electric Power Delivery System*.

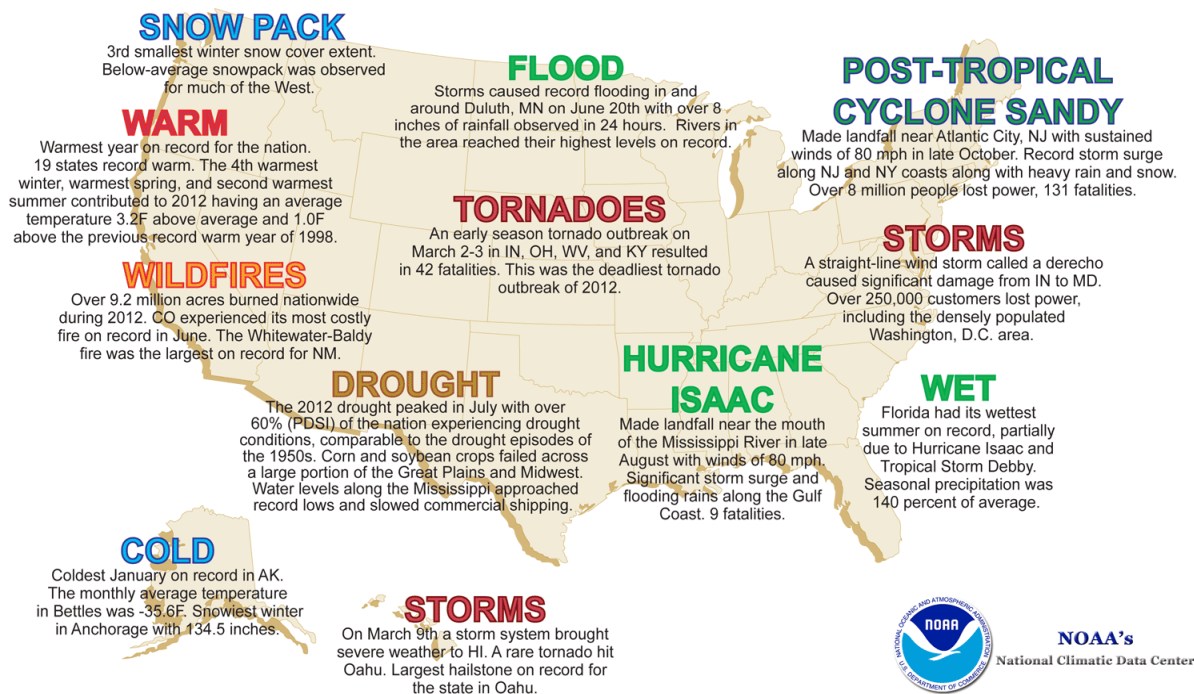


FIGURE 1-1 Preliminary significant U.S. weather and climate events for 2012. SOURCE: NOAA National Climatic Data Center, *State of the Climate: National Overview for Annual 2012*, available at <http://www.ncdc.noaa.gov/sotc/national/2012/13>.

Patricia Hoffman, Assistant Secretary for Electricity Delivery and Energy Reliability in the Department of Energy (DOE), also urged a broader view of climate impacts, noting the wide array of weather-related incidents just last year across the entire United States, including widespread drought in Texas and the Southwest, record low temperatures in the Northwest, and wildfires across the West (see Figure 1-1). Dr. Hoffman also pointed out that thousands of weather records had been broken across the United States in the past year, and these trends are likely to continue. Electricity generation sources have already been impacted by drought, with low water levels forcing some power plants to reduce capacity because of limited cooling power. Further impacts to the electricity system are anticipated. The question, according to Dr. Galloway, is whether events like Sandy can create a teachable moment for those parts of the country that have not yet had extensive experience with extreme weather events.

Given this shifting landscape, identifying vulnerabilities in the electric power system to both natural disasters and terrorist attacks remains a serious challenge. Chapters 2 and 3 are focused on physical vulnerabilities in the system and issues of cybersecurity, respectively, in order to better understand the threats to resilience that the electric power system faces. Chapter 4 then addresses how communities respond to outages, while Chapter 5 details future developments of the grid that impact the resilience of the system as a whole. Chapter 6 provides an overall summary of the key points of the workshop.

2 Grid Infrastructure

To illustrate the complexity of the electric power delivery system, **Granger Morgan, CMU**, showed a diagram of a heavily interconnected system (Figure 2-1). Maintaining reliability of such a network requires significant coordination of resources. Such careful balance naturally introduces four vulnerabilities:

- Large, centralized power generation sources are often highlighted as potential targets for terrorists since the loss of a large generator would reduce electrical capacity by hundreds of gigawatts. However, as Dr. Morgan pointed out, these sources are heavily secured against all but very large terrorist attacks. Natural disasters are more likely threats, and most generators are susceptible to fuel disruptions.
- Transmission lines are easy targets for terrorists, but they are also easily replaced. However, natural disasters such as hurricanes and ice storms can also do serious damage to transmission lines.
- Substations, especially those with high-voltage transformers, are probably the most vulnerable to terrorist attack because they are essential components of the transmission system and would take a long time to replace.
- Control centers coordinate the operation of the grid to maintain reliability of the system. The loss of a control center, which is the brains of the system, can have a substantial impact on the operations of the electric grid. Much of the vulnerability of the control center is related to cybersecurity threats, which will be discussed in Chapter 3.

David Owens, Edison Electric Institute, noted that while much of the discussion is focused on the bulk power system, the most common challenges are at the distribution level, which can then end up affecting the bulk power system. He reiterated that substations and substation transformers are potential points of vulnerability in the system. According to **John Kassakian, Massachusetts Institute of Technology (MIT)**, substation attacks are a problem that can cause tremendous disruption, particularly if key lines are affected as in the case of a switching station. **Sarah Mahmood, DHS**, noted that the manufacturing lead time for a single, large transformer can be up to 18 months plus another 2-3 months to get it installed and operational. Reducing this downtime is the motivation for DHS's Recovery Transformer Program (RecX), which is discussed in great detail in Box 2-1. **Joseph McClelland, Federal Energy Regulatory Commission (FERC)**, noted that additional complications can arise from the specialization of transformers such as changes in energy efficiency, which can impact interchangeability and thereby reduce the number of spare units for a particular location.

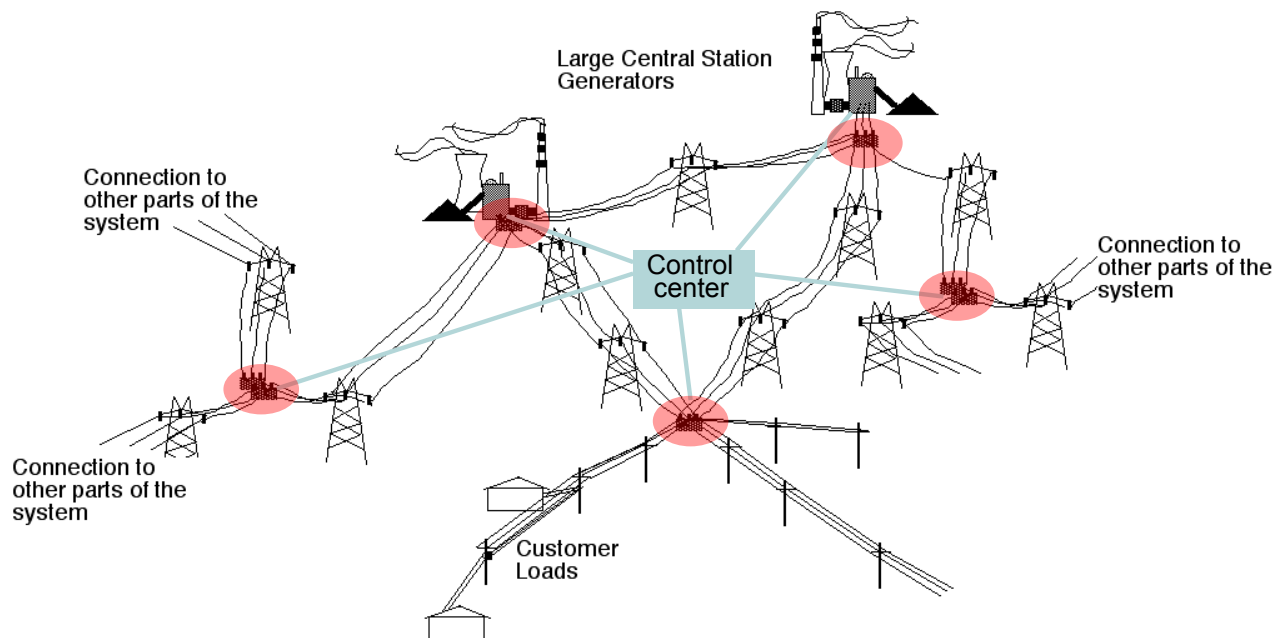


FIGURE 2-1 Illustration of the electric power delivery system. Substations are denoted by red ellipses. SOURCE: Adapted from graphic of Granger Morgan, Carnegie Mellon University, workshop presentation, February 27, 2013.

Ultimately, any of these vulnerabilities could lead to significant outages. **Daniel Bienstock, Columbia University**, detailed the ways in which one part of the network can have devastating impacts on the rest of the system, stressing segments that may not even be in proximity to each other. By studying the way in which small components affect the greater whole, Dr. Bienstock hopes to develop real-time control algorithms that can analyze a cascading blackout and, while perhaps not mitigating it fully, at least identify the measures to make it less disruptive. Using publicly available data for the Eastern Interconnect, he was able to show how one such control algorithm, in conjunction with fast-acting controls, could rapidly stabilize the blackout, reducing the number of line outages from almost 6,000 to just 11 for a particular initial outage. Such a combination of controls with real-time analytics is one way to dampen the impact of even a widespread terrorist attack.

Attacking the Infrastructure

The utilities are relatively well prepared for physical attacks on the grid infrastructure that are dispersed, uncoordinated, and limited according to **Dr. Kassakian**. As **William Ball, Southern Company Services**, noted, restoration procedures are well documented for an unplanned line or generator outage or a case where one or even two transformers or other equipment are affected (what are called “n-1” and “n-2” contingencies).

According to Dr. Kassakian, much more challenging is the case of a widespread coordinated attack. For instance, in the case of the 9/11 World Trade Center attack, there was a significant communications issue, as multiple agencies had different protocols that hindered a coordinated response. Furthermore, such an attack might take place across multiple nodes in the system,

which can result in the types of cascading blackouts mentioned previously. Such attacks also typically occur without warning, reducing opportunities for pre-emptive mitigation strategies. Transmission lines are vulnerable to air attack in numerous ways. He also pointed out that an attack on a switching station, which serves as an interconnect between multiple lines, might be just as disruptive as a coordinated attack.

One particularly damaging and coordinated attack could utilize the threat of an electromagnetic pulse (EMP) weapon. While there are some parallels to a geomagnetic disturbance such as the one that shut off power throughout the northern reaches of the United States and Canada on March 13, 1989, an EMP device has a far more localized and targeted impact. **Massoud Amin, University of Minnesota, and Dr. Kassakian** both noted that an EMP weapon, which could be as small as a briefcase, could be used to attack the control systems of the grid at the same time as an attack on the physical infrastructure, thus significantly compounding the effect of the physical attack by disabling some of the inherent balancing mechanisms in the grid. A cyberattack combined with a physical attack on the infrastructure may have a similarly crippling effect, as is discussed in Chapter 3.

Natural Disasters

As **Steve Whitley, New York Independent System Operator (NYISO)**, noted, however, nature can launch its own devastating, widespread attack. While utilities may typically be prepared for an “n-1” or “n-2” event, Mr. Whitley noted that Hurricane Sandy was an “n-90” event. Long Island lost all ties to Connecticut and New Jersey, and New York City lost all ties to New Jersey (Figure 2-2). Over 8 GW of generation capacity went offline, both through loss of transmission and, more directly, through flooding, resulting in over 2 million customer outages in the immediate aftermath.

However, Mr. Whitley pointed out that Hurricane Sandy proved that there were a number of things that had been done to mitigate the impacts on NYISO’s customers. Because of the advance warning, regular transmission line maintenance had been cancelled, and generators on planned maintenance outages were recalled so that they could be immediately put to best use immediately following the storm. Furthermore, by contacting other grid operators in the region, it was possible to coordinate possible responses to outages and ensure that everyone in the affected area could be on the same page.

During the storm, Mr. Whitley noted the difficulty of maintaining integrity of the interconnected system; however, because declining customer load coincided with a

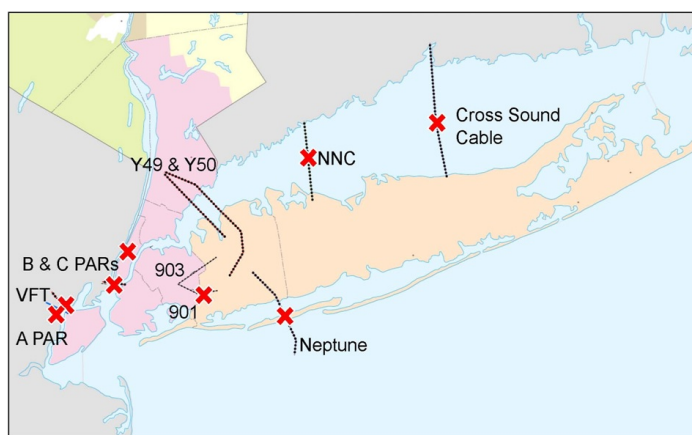


FIGURE 2-2 Interconnections in the New York/New Jersey area after Hurricane Sandy. A red X denotes an outage. SOURCE: Steve Whitley, NYISO, workshop presentation, February 28, 2013.

simultaneous loss of generation capacity, it did ease efforts to maintain 60 Hz in the regions that did not lose power. Such regions were also helped by New York City's requirements for local generation and blackstart capability, which is further discussed in Chapter 4. Throughout the recovery period as well, NYISO and the rest of New York's utilities were able to operate within power transfer limits, and communications and computer systems worked properly throughout the ordeal.

Solutions

Mr. Whitley, in recapping the implications of the Hurricane Sandy experience for the New York power grid, noted that with such potential for devastation of the physical infrastructure of the grid in the wake of natural disasters and terrorist attacks, it is important to recognize the potential for lessons learned and what can be done moving forward to improve the resilience of the system. Above all, a frequent theme by participants was simply the importance of planning—communication and action protocols are critical. And Mr. Whitley quoted Abraham Lincoln: “Give me six hours to chop down a tree, and I will spend the first four sharpening the axe.” This theme emerged across all aspects of resilience.

Particular to the physical infrastructure, one major concern was the susceptibility of substations to terrorist attack. **Dr. Kassakian** pointed to the need for additional security measures and possible physical hardening beyond a simple fence to reduce substation vulnerability; a recent working group of the Institute of Electrical and Electronics Engineers (IEEE) is developing a standard for such security measures, including facility monitoring and improved access protocols to deter intrusion. However, as Dr. Kassakian pointed out, while such deterrence may limit access, it is optimal to have a system robust to substation failure because it is impossible to secure every facility against a physical attack.

The use of a spare recovery transformer was seized upon by many in attendance as a serious option to reduce the vulnerability of the system to failed equipment. While the components of a substation are relatively easily replaced, the difficulty of and lead time necessary for replacing a transformer is a hindrance that can slow down the mitigation response. **Anjan Bose, Washington State University**, currently on leave and serving on the Department of Energy's Grid Tech Team, did mention that the recent rebirth of transformer manufacturing in the United States, as described by Mr. Ball, does reduce the amount of downtime a utility might expect for replacement. However, it was the achievements of the DHS RecX program (Box 2-1) presented by Ms. Mahmood that truly represented a significant step forward in this area. **Richard Schuler, Cornell University**, noted that if these transformers truly are a comparable economic investment, it should not be an impediment for many state commissions. He added that because the industry commonly subsidizes public goods, having this redundancy seems like an obvious and worthwhile investment. **Jay Apt, CMU**, did point out that a number of organizations at this point remain underinformed about the developments of the RecX program, and **Dr. Amin** expressed concern about a lag of as much as 10 years for these transformers to get out to industry given the timeline of development thus far.

BOX 2-1**The Department of Homeland Security Recovery Transformer Program**

Sarah Mahmood, Department of Homeland Security, described the successful deployment of a recovery transformer outside Houston, Texas. The RecX recovery transformer program is designed to act as a rapidly deployable spare for a 365 kV:138 kV/200 MVA transformer, reducing the amount of time for transport and installation from 2 or 3 months down to about a week. The key design feature is to replace the three-phase transformer with three single-phase transformers. Each is smaller and weighs much less than a full three-phase transformer, allowing it to be delivered by truck rather than train or barge. While the transport of the transformer requires state permitting in advance, the convoy design enables rapid installation by transferring its oil, cooling equipment, and other ancillary equipment (control cabinets, bushings, etc.) along with the transformer. Part of the rapidity of installation also stems from the use of an MA65 trailer, which is analogous to a Schnabel car in design and allowed for the rapid positioning of the transformer at the CenterPoint substation. In addition, the standard modular design could be manufactured much more quickly than large custom-designed transformers.

Although the RecX recovery transformer was initially designed to be a spare that would be replaced after 2-3 years, extensive testing has proven the reliability and efficiency of the transformer to be comparable to a typical 365:138 transformer. Furthermore, at \$7.5 million, the price of the RecX transformer is on a par with other 365:138 transformers on the market (\$6 million to \$10 million), which means that a utility could consider this as part of its sparing strategy. Currently, DHS is focused on outreach to get stakeholders RecX-certified.

Paul Parfomak, Congressional Research Service, remarked that there had been significant concern for the replacement of larger transformers, but Ms. Mahmood replied that the basic design for this transformer *is* applicable to the larger 500 kV and 765 kV classes of transformer as well. However, because there is no longer funding for the RecX program, replacements for these larger transformers are not being developed at this time. Until those transformers are designed, the highest capacity part of the transmission system is still vulnerable to long-term outages. There was a further question about the susceptibility of these transformers to attack—while Ms. Mahmood agreed that these transformers are just as susceptible to a physical attack as those they replaced, the RecX transformer is slightly less susceptible to ground-induced currents and, therefore, EMP weapons.

A final strategy to improve the resilience of the physical infrastructure is improved use of a synchrophasor network, as suggested by both Dr. Bienstock and Dr. Kassakian. According to Dr. Kassakian, real-time measurements of the grid using a synchrophasor network could enable better control of the load, which is of particular concern during outages involving large portions of the system. This is similar to the arguments of Dr. Bienstock, who illustrated the effectiveness of real-time control algorithms in the case of multiple line failures. In his example, such algorithms limited the cascading losses to 11 outaged lines and 25.5 percent yield as compared to the case without such controls (39.3 percent lost yield and 5,959 outaged lines). However, Dr. Kassakian highlighted the complexity of the problem as well as the resources and timescales involved, noting that such real-time control was only in the demonstration stage in limited regions of the country and was not likely to be widely deployed in the near future.



3

Cybersecurity of the Grid

In order to provide more reliable and efficient service, the electric power delivery system is incorporating an ever increasing amount of data transfer, with communications occurring over a wide array of systems. **Massoud Amin, University of Minnesota**, noted that the systems have become so intertwined that operators may forget where the data is coming from, citing an anecdote of a power plant operator who was receiving all of his commands over the internet. **Granger Morgan, CMU**, pointed out that while adding more points of intelligent control can add capacity, stability, and flexibility, it also adds more entry points for cyberattack. **Paul Nielsen, Software Engineering Institute, CMU**, asked a question about the conundrum facing utilities today: What risk are you willing to accept for capability?

While the sophistication of cyberattacks is increasing, the level of technical knowledge necessary for the attack is decreasing according to both Dr. Nielsen and **Patricia Hoffman, DOE** (Figure 3-1). **Joseph McClelland, FERC**, noted that the power sector is an increasing target for cyberattacks, both in the United States and abroad. Stressing the ubiquitous nature of cyberattacks, **Terry Boston, PJM Interconnection**, recalled a common saying: “There are two types of people: those who’ve been attacked, and those who don’t know they’ve been attacked.” With such attacks becoming commonplace, it is crucial to understand where the underlying vulnerabilities lie in the electric power delivery system.

Merging of Infrastructures

Galen Rasche, Electric Power Research Institute (EPRI), described the new world that is emerging—just as critical infrastructure has become increasingly integrated with the electric power system, so too has the grid become more reliant upon the communications network (Figure 3-2). An increasing number of sensors applied to the grid allows for both improved flexibility and increasing automation. However, Mr. McClelland noted that such an increase in automation increases the number of on-ramps for cyberattacks. And as Mr. Rasche pointed out, this increased integration with the communications infrastructure can leave the grid vulnerable, as layer upon layer of connectedness results in an increasing amount of trust placed in suppliers.

The legacy systems common in transmission and distribution systems often communicate via insecure protocols, according to Mr. Rasche. One of the biggest challenges in securing this legacy hardware is the fact that these very protocols are created through standards organizations, and such processes are, by design, very slow to change. Therefore, more robust network, system, and security management protocols are necessary for transmission and distribution systems to identify the types of security faults common to antiquated hardware.

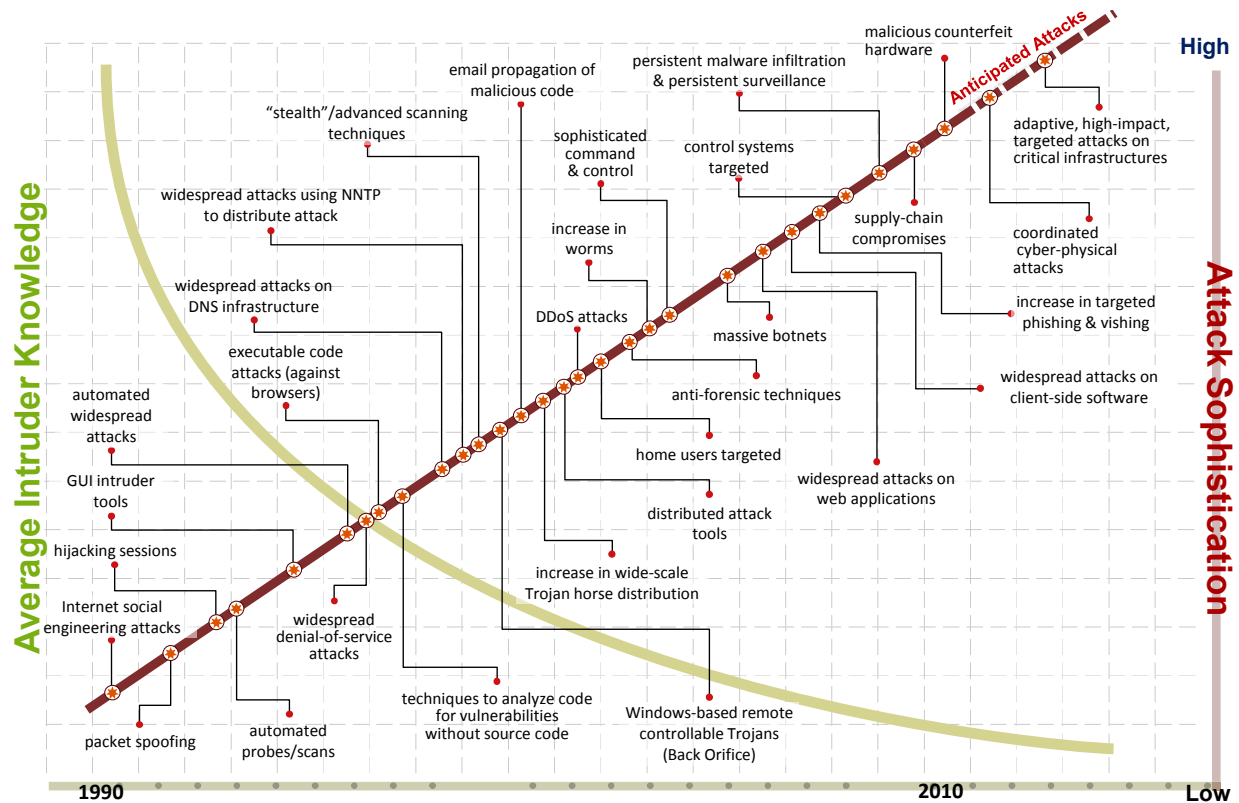


FIGURE 3-1 Average intruder knowledge and attack sophistication as a function of time. SOURCE: Presented at the workshop by Patricia Hoffman, Department of Energy, February 27, 2013; from Howard Lipson, Carnegie Mellon University (CMU) Software Engineering Institute CERT®. Copyright 1998-2011. This CMU and Software Engineering Institute material is furnished on an “as-is” basis. CMU makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. CMU does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

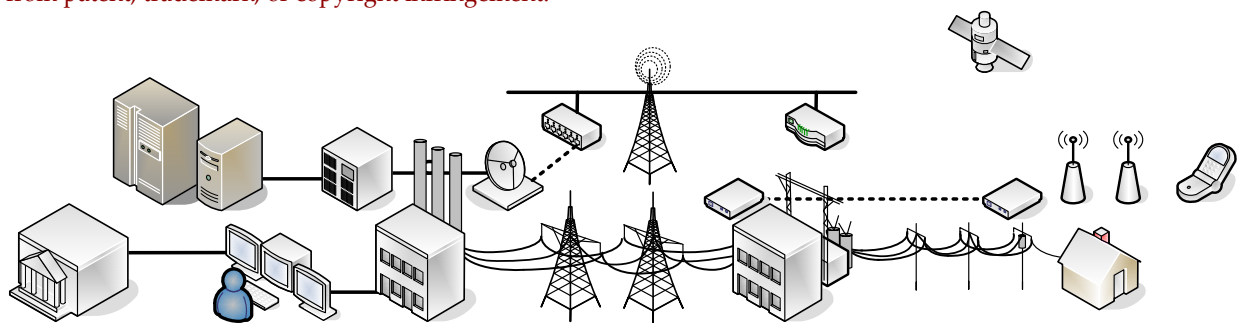


FIGURE 3-2 The communications network (top) and electric grid infrastructure (bottom) merged, with smart metering being deployed in homes, sensors being deployed at the distribution infrastructure, and all of this being communicated to users at central control facilities. SOURCE: Galen Rasche, EPRI, workshop presentation, February 27, 2013.

Modernized hardware and software do not necessarily offer increased protection, however. As **Fred Hintermeister**, North American Electricity Reliability Corporation (NERC), pointed out, supply chain security is critical to ensuring that a particular subsystem is secure, regardless of the system or vendor. **Dr. Nielsen** agreed, expanding on the necessity of knowing who wrote the software for every component of all of your partners’ systems. While this may seem a

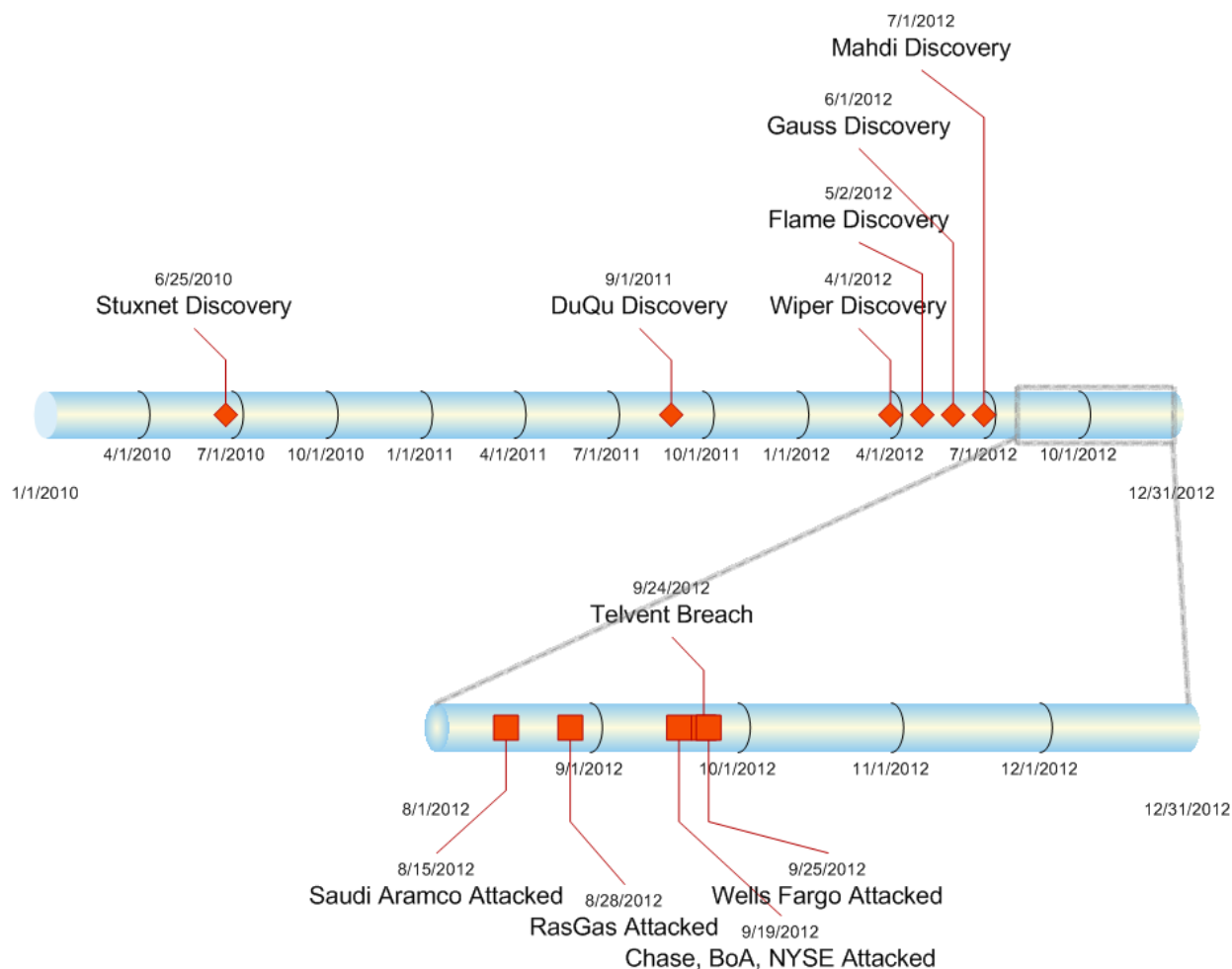


FIGURE 3-3 High-profile cyberattacks (2010-2012), with magnification of August through December, 2012. SOURCE: Fred Hintermeister, NERC, workshop presentation, February 27, 2013.

daunting task, the increasing number of attacks is pushing hard on utilities and their partners to ensure that their systems are secure at every level. NERC is working with a global network of governmental intelligence sources, vulnerability researchers, and others to develop products that specifically address emergent issues, particularly in the area of cybersecurity. A system is only as secure as its weakest link, and it is a crucial part of established NERC procedure to push mitigation measures out to the relevant bulk power system entities in a timely manner so that they may address the full chain of operations.

Risk Assessment and Cybersecurity

Given the prevalence of attacks (Figure 3-3), it is crucial to evaluate how best to maintain system integrity with minimal risk. Dr. Nielsen suggested that appropriate choice of architecture can help make these trades in design by linking the business goals to system goals. **Dr. Morgan** noted that that separate risk assessments could be needed for natural disasters and intelligent agents. While it would be possible to evaluate which architecture is more vulnerable

than another to a given susceptibility, the probability of attack relevant to making an analytical choice in system architecture will be substantially different for a natural disaster than for a terrorist threat.

Making such a risk assessment is difficult, according to **Mr. Rasche**. Because cybersecurity involves the meshing of two networks based on completely different expertise, it is difficult to adopt common protocols for risk analysis. **Narain Hingorani, Consultant and National Academy of Engineering member, and Anjan Bose, Washington State University**, agreed that cross-expertise and operator training are both significant issues at this interface. **Mr. Hintermeister** mentioned ongoing work in this area: The NERC Information Sharing and Analysis Center maintains a near-real-time, grid-common operational picture to inform risk assessment and mitigation development and delivery.

Diane Munns, MidAmerican Energy Company, noted that the regulatory bodies are at a particular disadvantage when it comes to both expertise and authority. On top of this, the regulatory process itself is not well designed for cybersecurity, according to **Mr. McClelland**. NERC can develop standards for reliability and cybersecurity and submit them to FERC, but because the process is both slow and open, it is not adequate for national security purposes—in effect, both the threat and the mitigation strategy are announced through the regulatory process.

Given the nature of the cyberthreat, there was significant discussion over the potential for catastrophic damage, particularly for causing damage to the physical infrastructure. Dr. Morgan cited recent work at Carnegie Mellon indicating a low probability that a hacker could destabilize the bulk power grid by toggling customer loads via hacked smart meters.¹ However, Mr. McClelland cited both the Aurora test at Idaho National Laboratory² and a collaborative project with Lawrence Berkeley National Laboratory to identify critical frequency vulnerabilities for customer load shedding as evidence of the sensitivity of certain aspects of the physical infrastructure to cyberattack.³ Dr. Amin also suggested such potential vulnerability, though other participants commented that the Aurora experiment in particular was not indicative of a typical utility control system. Regardless of the disagreement over a potential causal link, however, participants from both perspectives agreed that a cyberattack combined with a damaged physical infrastructure would magnify the effectiveness of a terrorist threat, particularly in the event of a coordinated attack on multiple fronts.

Solutions

There are many cybersecurity actions that can be taken to reduce vulnerability to a cyberattack. Most obviously, according to **Dr. Amin**, wireless and public internet access should

¹ A. Narayanan, 2012, The emerging smart grid: Opportunities for increased system reliability and potential security risks, Dissertations, Paper 138, available at <http://repository.cmu.edu/dissertations/138>.

² Video available at <http://www.youtube.com/watch?v=fJyWngDco3g>.

³ J. H. Eto, J. Undrill, P. Mackin, R. Daschmans, B. Williams, B. Haney, R. Hunt, J. Ellis, H. Illian, C. Martinez, M. O'Malley, K. Coughlin, and K. Hamachi-LaCommare, 2010, Use of frequency response metrics to assess the planning and operating requirements for reliable integration of variable renewable generation, LBNL-4142E, December, available at <http://certs.lbl.gov/pdf/lbnl-4142e.pdf>.

be avoided at all costs. **Mr. Boston** suggested building the system like a nuclear secure lab, where communication is handled as an information diode that does not “shake hands” with the computer, so that information transfer is one-way.

According to Dr. Amin, the vulnerabilities of centralized control seem to demand smaller, local system configurations. Thus, resilience may depend upon the ability to bridge top-down and bottom-up decision making in real time. This highlights the need for building secure sensing, fast reconfiguration, and self-healing into the infrastructure. **Mr. Rasche** also recognized the importance of real-time analytics and integrity checking, because these systems cannot simply be taken off-line. Mr. McClelland highlighted the ongoing efforts by FERC to anticipate attacks through pattern recognition as one particular example of real-time analytics that can increase cybersecurity in the power system. **Ms. Hoffman** also acknowledged the importance of situational awareness: Aggregating monitoring information to develop a “common operating picture” enables real-time prevention and can boost the effectiveness of training exercises. Such an approach should be risk-oriented and data-driven, with the data being linked to actionable knowledge, according to **Mr. Hintermeister**.

Tabletop exercises on the impact of cyberattacks offer an opportunity for close coordination between information technology experts and power system experts, according to **Mr. Rasche**. Such penetration testing would be significantly improved through a common metric for cyberresilience. Assessing the vulnerability of a system is difficult, particularly in the case of a zero-day, or previously unknown, vulnerability. How can one measure resilience to an unanticipated event?

Because most utilities do not have an integrated security system, according to Mr. Rasche, devices tend to be upgraded in silos. A more systematic approach would allow correlating events across distributed power systems with the data being collected, as suggested above. **Dr. Amin** suggested that the industry should facilitate and encourage design of security at the start and look to include it in standards where appropriate. The certification of vendor products for cyberreadiness would essentially allow for security by default. Mr. Hintermeister pointed out the use of NERC’s HYDRA network of subject matter experts for the technology vendor supply chain. Because reliable operation necessitates security throughout the entire supply chain, it is crucial to approach the problem at both the hardware and software level.

Mr. Boston pointed out that collaboration is key. It is important to leverage industry relationships to share best practices and coordinate response plans. He pointed to the benefits of PJM Interconnections partnerships with DHS, the University of Maryland, Boeing, and the Pacific Northwest National Laboratory as evidence of the way in which shared expertise can benefit the industry. While Mr. Hintermeister agreed on the need to embrace partnerships, he stressed that it is important to have empathy for the partners. Everyone has a different role and different concerns, and one must be aware of those additional requirements.



4

Responding to Outages

Though much of the workshop focused on what to do to prevent future outages, **Jay Apt, CMU**, observed that despite the best efforts of extremely talented power engineers, blackouts will continue to happen, which means that the resilience of the system will inevitably be dependent not just on reducing the number of outages but also on how the system responds to them. Large blackouts can be particularly devastating and happen much more frequently than a normal distribution predicts. Therefore, **Clark Gellings, EPRI**, asked the central question: How resilient is the grid to high-impact, low-frequency events?

Restoration of Power

Mike Adibi, IRD Corp., pointed out that the impact of a blackout exponentially increases with the duration of the blackout, and the duration of restoration decreases exponentially with the availability of initial sources of power. For several time-critical loads, quick restoration (minutes rather than hours or even days) is crucial. Blackstart generators,¹ which can be started without any connection to the grid, are a key element in restoring service after a widespread outage. These initial sources of power include pump-storage hydropower, which can take 5-10 minutes to start, to certain types of combustion turbines, which take on the order of hours. According to Mr. Adibi, automated operation of these generators is more likely to be successful than manual operation; however, he noted that a “conservative operating philosophy” has limited the deployment of devices enabling automatic blackstart operation.

There was some question as to whether requirements of NERC for blackstart generation are sufficient. **Mr. Whitley, NYISO**, has found that they serve his customers well thus far. Typically, the level of blackstart operation is based on past experience; however, moving forward there may be some challenges owing to reduced reserve margins from phasing out older generators. Mr. Adibi felt that it is not sufficient to simply set a reserve for the system but that it is important to divide the grid into its respective subsystems and determine whether there is sufficient reserve for these subsystems as well.

¹ A blackstart resource is defined as “a generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator’s restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator’s restoration plan.” See **Glossary of Terms Used in NERC Reliability Standards**.



FIGURE 4-1 Center Point Energy personnel repair a downed power line (Houston, TX, September 23, 2005). Utility companies were out early to repair damage caused by Hurricane Rita. SOURCE: Ed Edahl, FEMA.

Beyond the challenge of generator response, there is also a concern for the distribution system, which was touched upon in Chapter 2. **John Kassakian, MIT**, pointed out that it is crucial to think about the challenges of both restoration *and* repair. For a limited outage, restoration can be rapid, which will then allow sufficient time for repair to bring the system to full operability, although there may be a challenge for subsurface cables in metropolitan areas. On the other hand, in widespread outages, restoration itself may be a significant barrier, as was the case in the 1965 and 2003 Northeast blackouts. Natural disasters, however, can also lead to significant issues of repair—after Hurricanes Rita and Katrina, full repair of the electric power system took several years (Figure 4-1). In the case of Hurricane Sandy, David Owens, Edison Electric Institute, and William Ball, Southern Company Services, both pointed out that granting first-responder status to the utilities enabled more rapid response than would occur under normal conditions, which is one way to improve restoration time at the local level.

Critical Services and Community Resilience

Gerald Galloway, University of Maryland, pointed out that economic and social systems are becoming increasingly interdependent. **Massoud Amin, University of Minnesota**, noted that this interconnectedness is one of the major reasons the electrical grid is an attractive target for terrorist attack—namely, other services have become dependent on the electric power system. **David Kaufman, FEMA**, recognized that impacts of overlapping interdependency could cascade because the supply chain for many industries has become globalized—for

example, according to Mr. Kaufman, truck production in Louisiana was shut down by the earthquake in Japan, which halted the supply of a particular mineral needed for metallic paint. Thus, evaluating resilience in response to a power outage goes far beyond the electric power sector.

Resilience and Risk

According to a recent NRC report,² resilience is “the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events.” Dr. Apt noted that the services critical to a community are diverse, including elevators, subways, traffic signals, police stations, cell phone towers, grocery stores, ATMs, and gas stations. **Joseph McClelland, FERC**, pointed out that not only does the electric power system feed into these services, but in some cases it is reliant on these systems as well. For instance, with a shift in generation fuel from coal to natural gas, the energy sector is increasingly reliant on the natural gas pipeline infrastructure; with events like the Telvent compromise in 2012³ and the Shamoon cyberattack in 2012⁴ in Saudi Arabia and Qatar, resilience to terrorism and natural disaster for the electric power system involves both upstream and downstream dependencies. The natural gas system may be particularly stressed during the winter when it is being used for heating, making the system especially vulnerable to attack. As **Susan Tierney, Analysis Group, LLC**, pointed out, it is important to view the electric power delivery system in an integrated way: How are the systems of governance and communities of interest affected by the operation of the grid?

Because risk cannot be completely eliminated, residual risk must be effectively managed according to Dr. Galloway. Much of the work in this area has tended to be based on anecdotal response, and there was significant discussion at the workshop on how to organize these responses in a controlled, systemic way. Currently, a community finds out it is vulnerable when a storm hits, which is obviously suboptimal. Mr. Kaufman agreed, noting that current models of risk assessment are based largely on historical record. Given the shifting environment of the electricity delivery system and the interdependencies among a number of infrastructures,



² National Research Council, 2012, *Disaster Resilience: A National Imperative*, The National Academies Press, Washington, D.C.

³ Telvent Canada is a company that provides remote administration and monitoring tools for the energy sector. In September 2012, the company discovered that its internal firewall and security system had been breached by a Chinese hacking group.

⁴ Shamoon is a computer virus capable of transmitting information about the files of the infected computer as well as deleting all data from the hard drive. It was first used on August 15, 2012, by hackers from a group called the Cutting Sword of Justice in an attack on Saudi Arabia’s national oil company, Aramco. It was also suspected in a later cyberattack on a large liquefied natural gas company in Qatar, RasGas.

this methodology not only likely underestimates today's risks, but it is also grossly inadequate for future projects. **Miles Keogh, National Association of Regulatory Utility Commissioners**, pointed out that there is always a component of residual risk to be managed, and it is crucial for regulators to determine precisely where such risk may be acceptable. Ways of identifying and prioritizing such risk were, however, not discussed at the workshop.

Coordination and Engagement

Mr. Kaufman acknowledged that there is a tremendous amount of ongoing effort to improve community resilience; however, how to engage regulators and other interested parties is unclear. At the community level, planning tends to occur at the "last mile of distribution," which Mr. Kaufman found appropriate, but on a broader regional scale, the "strategic capacity," or "wholesale," level of planning is not filling in. According to **Dr. Tierney**, there is a significant amount of siloing that restricts the engagement of the relevant regulatory authorities. In a recent discussion of community resilience to power outages in Massachusetts, she observed that there was a quick segmentation into things like emergency generators, responsive backup, and the like.

Various agencies are involved in these issues, but to date it is unclear who is ultimately responsible for coordination and response, which was the central focus of the Massachusetts planning meeting attended by **Dr. Tierney**. The agencies might include state emergency management offices; state energy offices, who handle issues such as fuel coordination and waivers for moving product; the public utility commission, which is a rate-setting body; the utilities themselves; fuel operators, which are an unregulated community; standards-setting bodies for reliability at both the federal and local levels (FERC and NERC, respectively); and DHS, which includes FEMA. Mr. Kaufman discussed the role of FEMA in response to Hurricane Sandy to illustrate current federal efforts (Box 4-1).

Despite the breadth of these actors, none of them have any authority except to enlist the involvement of institutions such as hospitals, banks, and police and fire departments, all of which provide critical services for the community. Thus, according to Dr. Tierney, it is difficult to determine what an appropriate role for governance is: How do we think about offering encouragement for participation, and what is a prudent role for the utilities and the utility commissioners? An added complication with any engagement is that much of the information necessary to make good decisions is classified and/or proprietary, but any such decision-making needs to be made in the public domain. While there is some agreement to engage in this process under the idea of adaptation, particularly in response to natural disasters and climate change, Dr. Tierney found it problematic to disseminate the best practices for outreach to the relevant parties.

Solutions

Given the broad scope of resilience, there are a number of areas where action can be taken to improve future responses to natural disasters and terrorist attacks. **Patricia Hoffman, DOE**,

BOX 4-1

Responding to a Crisis: Hurricane Sandy

David Kaufman, Federal Emergency Management Agency, discussed recent government involvement in response to Hurricane Sandy as an illustration of the current level of community engagement. FEMA was involved in two major issues in response to Sandy, the fuel sector and the power sector. In the case of fuel, Mr. Kaufman noted that FEMA was largely responding to developing symptoms instead of addressing a central cause. This led to a focus on how fuel is distributed to the marketplace. In the case of power, FEMA convened calls with major utilities in impacted areas. The agency also mobilized federal military air assets to fly crews to impact areas, though this was a small fraction of the overall utility response. Mr. Kaufman found that because of FEMA's limited resources, government response was meant not as the main actor but as an accelerant to engage the relevant local groups such as utilities and other service providers. The question then becomes what these relevant industries need from government in order to meet local demand and to then build resilience in those systems.

noted that improvements to facilities related to industries that interact with the electric power system could provide increased resilience. Establishing standards and guidelines for fuels facilities, revising current building and rehabilitation codes, and developing alternative system configurations for critical facilities all harden the infrastructure, which could improve resilience to widespread outages. **Fred Hintermeister, NERC**, noted that the electric power industry is the only industry (apart from nuclear) with mandatory and enforceable critical infrastructure protection standards.

Dr. Galloway stressed a proactive approach as well, noting that building resilience will be more effective in reducing losses of life, property, and economic productivity than other current approaches. This was discussed at length in the NRC report *Disaster Resilience: A National Imperative*.⁵ Dr. Galloway cited an example from Cedar Rapids, Iowa—in 2008, the town was able to evacuate quickly in response to an unforeseen flood due to the years of preparation for evacuation that it had practiced out of fear of an accident in a nearby nuclear plant. While community resilience does begin with strong local capacity, Dr. Galloway emphasized that a top-down “culture of resilience” approach could address some of the issues of consistency and coordination (Box 4-2). Policies designed to improve national resilience must also take the long-term view to help avoid short-term expedients that can diminish resilience. For example, some policies allow levees to be rebuilt only to the same level as before they were damaged, but not to be improved.

Ms. Hoffman cautioned that a national resilience policy should not mean “one size fits all”—each area of the country has its own strengths and its own risks. **Mr. Kaufman** agreed,

⁵ National Research Council, 2012, *Disaster Resilience: A National Imperative*.

BOX 4-2

Characteristics of a Resilient Nation in 2030

- Individuals and communities are their own first line of defense against disasters.
- National leadership in resilience exists throughout federal agencies and Congress.
 - Community-led resilience efforts receive federal, state, and regional investment and support.
 - Site-specific risk information is readily available, transparent, and effectively communicated.
 - Zoning ordinances are enacted and enforced. Building codes and retrofit standards are widely adopted and enforced.
 - A significant proportion of post-disaster recovery is funded through private capital and insurance payouts.
 - Insurance premiums are risk based.
 - Community coalitions have contingency plans to provide service particularly to the most vulnerable populations during recovery.
 - Post-disaster recovery is accelerated by infrastructure redundancy and upgrades.

SOURCE: National Research Council, 2012, *Disaster Resilience: A National Imperative*, The National Academies Press, Washington, D.C.

challenging the common notion that massive disasters primarily occur along the coasts. According to Mr. Kaufman, the most expensive issue FEMA has been dealing with lately is flooding, but then many of those same areas have successively been dealing with drought. Any such plan should thus recognize that these are systemic issues.

A number of attendees noted how better data sharing could play a role in enhancing community resilience. **Dr. Galloway** felt that a significant amount of relevant data is hidden from the public, and that it was important to rethink what data is truly worth classification. **Mr. Ball** did note that the discussions in the power sector are often by necessity going on “below the radar” in a classified setting. Dr. Galloway felt that such data issues can inhibit the ability of workers on the ground to communicate results effectively to decision-makers so that they can be aggregated in a meaningful way. Although they may be useful, tabletop exercises often may not actually handle the underlying problems. **Dr. Tierney** stressed that the open sharing of best practices would offer significant aid to those areas that have not yet been hit.

Mr. Gellings suggested that it may be possible to leverage new technologies to ensure the continuation of essential missions, even after the grid has failed. One example cited was a light-emitting-diode traffic light paired with photovoltaics and battery storage, which would allow traffic lights to operate even without a connection to the bulk power system. Photovoltaics could also be used to provide solar chargers for cell phones, thus improving the resilience of the communications system, which is obviously heavily reliant on the electric power system.

According to Mr. Gellings, breaker panels are currently being designed that could respond to a photovoltaic array, enabling a customer to select which panels are turned on in a home and run directly from the photovoltaic array when the system is disconnected from the grid.

Granger Morgan, CMU, also stressed the potential impacts of distributed generation and microgrids. For example, in the case of heavily distributed generation, if there were ways to prioritize and select which customers to service, it would be possible to bring online through the distribution system just those components that are critical, such as police stations, ATMs, gas stations, or maybe even schools. Although this approach may not be effective in the case of a natural disaster that disables the distribution circuit (e.g., Hurricane Sandy), Dr. Morgan argued that in some scenarios at least part of the distribution circuit remains intact, capacity that could be used to make critical services far more resilient. This capability is discussed in further detail in Chapter 8 of *Terrorism and the Electric Power Delivery System*.⁶



⁶ National Research Council, 2012, *Terrorism and the Electric Power Delivery System*, The National Academies Press, Washington, D.C.

5

The Future of the Grid

Technologies discussed at the workshop could shape the electric grid in coming years. **Clark Gellings, EPRI**, noted that integrating new and existing technologies could address the issues of prevention, recovery, and survivability. Much of this focus is on distributed generation and smart grid technologies. **David Owens, Edison Electric Institute**, suggested that an important issue is how to ensure reliability, safety, and fairness, particularly in light of increasing renewable portfolio standards and public policy driving much of the emphasis on distributed generation.

Distributed Generation

Mr. Owens noted that distributed generation can offer stability but will require increased coordination. Currently, utilities look at very discrete customers with distributed power sources, but moving forward there is the potential for a much wider deployment of distributed generation, which could pose a challenge for reliability and safety as power flow becomes a two-way street. Mr. Gellings recognized that such change will be inevitable—the question is not whether more connection is going to happen but how best to adapt when it does (Figure 5-1).

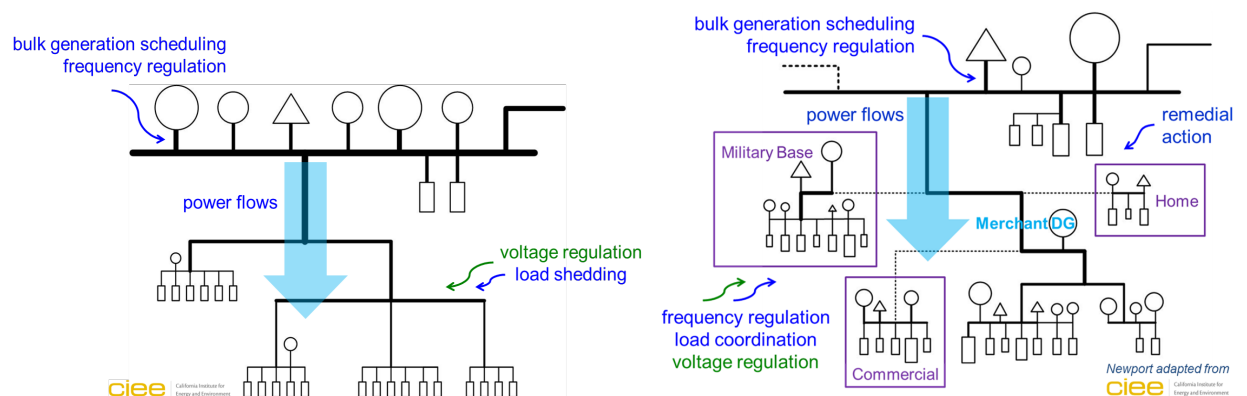
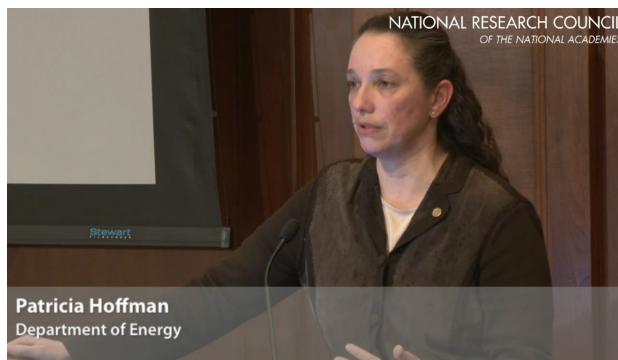


FIGURE 5-1 Operational evolution of the grid, showing a historical diagram of the typical grid structure from 1978 to 2001 (left) compared to the evolving grid structure incorporating microgrids (right). SOURCE: Adapted by Newport from the California Institute for Energy and Environment and presented by David Owens, Edison Electric Institute, February 27, 2013.

One audience participant asked why, if distributed generation is such a certainty, there is not currently a wider deployment of microgrids. **Granger Morgan, CMU**, pointed to issues with interconnections as well as evolving IEEE standards related to the issue of islanding; additional resilience is one of the benefits of a microgrid, but utilities are also concerned about safety issues with a partially activated system, according to Mr. Owens. There is also significant concern about funding and cost recovery—Mr. Owens pointed out that while there is an increased interest in improvements to the distribution system, much of the investment is falling on the utilities to ensure reliability and eliminate vulnerabilities associated with increased use of distributed generation. It is difficult to fairly account for these additional costs, many of which are coming under review by FERC and state PUCs. **Mr. Owens** cited net metering as one particular case that does not adequately account for the fact that a customer’s renewable generation from rooftop solar, for example, is not equivalent to power generated by the grid. **John Kassakian, MIT**, also pointed to renewable portfolio standards as a key cost burden being placed unfairly on utilities through public policy. **Dr. Morgan** noted that one policy prohibiting the existence of microgrids in some areas of the country involved exclusive service territory rules¹ and suggested examining the loosening of such rules to allow modest-size microgrids.



Because of an increasing focus on distributed sources of generation, energy storage is a particular issue of concern. **Patricia Hoffman, DOE**, pointed to work with Southern California Edison on an 8-MW Li-ion battery-based storage plant to complement a Tehachapi Pass wind farm as an example of ongoing research in this arena, noting that the evolving grid system needs to be thought about holistically.

The Smart Grid

Much of what has enabled distributed generation is related to smart grid technologies. **Anjan Bose, Washington State University**, noted that smart metering allows for consideration of distributed *load* as well as distributed generation. Dr. Bose suggested that the data currently being collected needs to feed into control systems. Mr. Owens pointed out that legacy distribution systems will have to be redeveloped to support such bi-directional and variable power flows safely and reliably.

In addition to greater real-time control, smart grid technologies can be used to reduce load through demand response. Ms. Hoffman pointed to a number of examples of utilities that have used smart grid technologies successfully. On the customer side, Oklahoma Gas and Electric

¹ K. Twaite, 2012, Monopoly money: Reaping the economic and environmental benefits of microgrids in exclusive utility service territories, *Vermont Law Review* 35:975-998, available at <http://lawreview.vermontlaw.edu/files/2012/02/twaite.pdf>.

was able to implement time-of-use and variable peak/critical peak pricing to reduce peak load by 30 percent. On the distribution side, automated circuit switches and sensor equipment implemented by the Electric Power Board of Chattanooga are estimated to have reduced customer outage minutes by 40 percent. And on the transmission side, 18 transmission owners within the Western Electricity Coordinating Council are installing and connecting 341 power management units and 62 power distribution centers to modernize transmission in the Western Interconnection. According to Ms. Hoffman, such implementation can enable a truly active distribution system that can be managed cost-effectively through a broad selection of technologies.

6

Summary of Main Points Raised in Workshop Discussions

Speakers and other participants discussed many interesting aspects of the committee's results, what has changed in recent years, and how lessons learned about the grid's resilience to terrorism could also be applied to threats from natural disasters. This chapter recaps points made by individuals at the workshop; none of the following statements should be construed as consensus findings, conclusions, or recommendations.

- Many workshop participants observed that *Terrorism and the Electric Power Delivery System*¹ is still relevant, although various participants identified notable developments since the report was written including a growing sophistication of cyber-attacks, improvement in the availability of replacement transformers, increased recognition of the significance of several high-profile natural disasters, and increased use of intermittent renewable energy technologies.
- There have been several high-profile natural disasters since the report was published. Although the report was written to address resilience of the power grid to terrorism, many similarities with resilience to natural disasters were identified by workshop participants. As noted, the apparently increasing frequency and severity of natural disasters are a further reason that reducing the vulnerability of the grid will be beneficial.
- The risk of outages, whether from terrorism or natural causes, cannot be eliminated, but some participants suggested ways that their frequency, extent, and duration could be reduced by making the system more robust, and the effects of catastrophes mitigated by advance planning and preparation.
- Industry participants, notably, advanced the view that the vulnerability of large power transformers at substations is still a major concern. Some noted that the loss of even one at a substation could incapacitate the substation until a replacement could be supplied, which could take months. Participants identified progress made by the Department of Homeland Security toward a standardized design recovery transformer but continued to express concern about the issue, observing that advanced planning can significantly reduce recovery time following a terrorist attack or major disaster such as Hurricane Sandy.
- Some participants observed that improved instrumentation and controls over power flow on the grid could reduce the extent of outages as well as facilitate the integration of renewable energy sources.
- Cyberattacks have become more frequent and more sophisticated since the report was written, and some participants noted that, as control of the grid becomes increasingly dispersed, the ability to resist and respond to cyber threats could depend on an increasing use of real-time

¹ National Research Council, 2012, *Terrorism and the Electric Power Delivery System*, The National Academies Press, Washington, D.C.

analytics, a secure supply chain, and redundant control centers. They observed, however, that all components of the control system must be built with high security, or the security of the entire system may be compromised. A number of workshop presentations that recapped ongoing efforts by NERC and the National Institute of Standards and Technology to develop a framework for supply chain security prompted some participants to conclude that while these efforts are beneficial overall, such efforts do not necessarily address how to identify key risk factors given a diverse set of system configurations.

- The workshop discussion of recent natural disasters such as Hurricanes Katrina and Sandy have exposed how crucial the electric power delivery system is for providing basic needs such as medical services and fuel. One participant suggested that understanding the threats posed by natural disasters and terrorist attacks requires a holistic view of risk assessment for both the grid and those sectors which rely on its services. Other participants noted that improving the resilience of critical service providers such as banks, gas stations, or hospitals may not fall directly within the electric power system's purview, but such projects may prove too costly for many industries to undertake on their own.

- Numerous workshop participants expressed concern over the depth of technical expertise available to many regulatory bodies, particularly as it pertains to cybersecurity and the range technical challenges affecting the performance of the power grid have developed in recent years, and the pace at which they are appearing. They observed that, without clear metrics for cybersecurity, in particular, it is difficult for regulatory agencies to understand the types of risk associated with different configurations and architectures of control systems and the value of protective measures.



Appendix A

Authorship of Terrorism and the Electric Power Delivery System

Committee on Enhancing the Robustness and Resilience of Future Electric Transmission and Distribution in the United States to Terrorist Attack

M. Granger Morgan, NAS,¹ Carnegie Mellon University, *Chair*
Massoud Amin, University of Minnesota
Edward V. Badolato,² Integrated Infrastructure Analytics, Inc.
William O. Ball, Southern Company Services
Anjan Bose, NAE,³ Washington State University
Clark W. Gellings, Electric Power Research Institute
Michehl R. Gent, North American Electric Reliability Corporation (retired)
Diane Munns, MidAmerican Energy Company
Sharon L. Nelson, State of Washington Attorney General's Office (retired)
David K. Owens, Edison Electric Institute
Louis L. Rana, Consolidated Edison Company (retired)
B. Don Russell, Jr., NAE, Texas A&M University
Richard E. Schuler, Cornell University
Philip R. Sharp, Resources for the Future
Carson Taylor, NAE, Bonneville Power Administration (retired)
Susan F. Tierney, Analysis Group, LLC
Vijay Vittal, NAE, Arizona State University
Paul Whitstock, Marsh, Inc.

Staff

Alan Crane, Study Director
Duncan Brown, Senior Program Officer
Harrison T. Pannella, Senior Program Officer (until July 2007)
James J. Zucchetto, Director, Board on Energy and Environmental Systems
Penelope Gibbs, Senior Program Associate

¹ National Academy of Sciences.

² The committee notes with regret Edward Badolato's death in November 2008.

³ National Academy of Engineering.

Appendix B

Workshop Participants

Invited Speakers

Mike Adibi, IRD Corp.
Jay Apt, Carnegie Mellon University
Daniel Bienstock, Columbia University
Terry Boston, PJM Interconnection
Gerry Galloway, University of Maryland
Fred Hintermeister, North American Energy Reliability Corporation
Patricia Hoffman, Department of Energy
John Kassakian, Massachusetts Institute of Technology
David Kaufman, Federal Emergency Management Agency
Miles Keogh, National Association of Regulatory Utility Commissioners
Sarah Mahmood, Department of Homeland Security
Joseph McClelland, Federal Energy Regulatory Commission
Paul Nielsen, Software Engineering Institute
Galen Rasche, Electric Power Research Institute
Steve Whitley, New York Independent System Operator

Committee on Enhancing the Robustness and Resilience of Future Electric Transmission and Distribution in the United States to Terrorist Attack

Massoud Amin, University of Minnesota
William Ball, Southern Company Services
Anjan Bose, Washington State University
Clark Gellings, Electric Power Research Institute
M. Granger Morgan, Carnegie Mellon University
Diane Munns, MidAmerican Energy Company
David Owens, Edison Electric Institute
Richard Schuler, Cornell University
Carson Taylor, Bonneville Power Administration (retired)
Susan F. Tierney, Analysis Group, LLC
Vijay Vittal, Arizona State University
Paul Whitstock, Marsh, Inc.

Workshop Attendees

Maria Amodio, ITTA
Paul Beaton, National Academy of Sciences
Gerald Blazey, Office of Science and Technology Policy
John Bobrowich, Wisconsin Energy Research Consortium
Mark Bryfogle, Anlage Research
Michelle Dallafior, Department of Energy
Jonathan DeVilbiss, U.S. Energy Information Administration
Tammy Dickinson, Office of Science and Technology Policy
Iris Ferguson, Department of Commerce
Louise Fickel, Department of Energy
Sue Gander, National Governors Association
Michael Gilmore, U.S. Government Accountability Office
Sherri Goodman, CNA
Barbara Granito, National Academy of Sciences
Sharon Grant, Carnegie Mellon University
Charles Gray, National Association of Regulatory Utility Commissioners
Tom Henneberg, Boeing BDS Ventures / Boeing Energy
Narain Hingorani, Consultant and National Academy of Engineering member
Michael Hsieh, Defense Advanced Research Projects Agency
Katie Jereza, Energetics, Inc.
Henry Kilpatrick, Econpolicy
Leanne Kuehne, Federal Energy Regulatory Commission
Vincent Le, Federal Energy Regulatory Commission
Mark Lively, Utility Economic Engineers
A.J. Maltenfort, i_SW Corporation
Ellory Matzner, Institute for Defense Analysis-Science and Technology Policy Institute
Ed May, Itron
Lamine Mili, Virginia Polytechnic Institute and State University
Paul Mohler, Law Offices of Paul B. Mohler PLC
Paul Parfomak, Congressional Research Service
Barbara Pope, The National Academies
Chris Schepis, House Committee on Homeland Security
Julian Silk, University of Maryland-College Park
Terrell Smith, The National Academies
Andrea Spring, Federal Energy Regulatory Commission
Sam Taylor, National Academy of Sciences
R. Cornell Teague, House Appropriations Committee-Homeland Security
Mitzi Wertheim, Naval Postgraduate School
Greg Wilshusen, U.S. Government Accountability Office
Orhan Yildiz, U.S. Energy Information Administration

Appendix C

Workshop Presentations and Discussions

Wednesday, February 27, 2013

Welcome

Ralph Cicerone, President, National Academy of Sciences

Peter Blair, Executive Director, Division on Engineering and Physical Sciences, National Research Council

Review of Terrorism and the Electric Power Delivery System

Granger Morgan, Carnegie Mellon University (NRC Panel Chair) - Presentation

Current and Future Needs for the Electric Power Delivery System

Panel Discussion

Massoud Amin, University of Minnesota (cyber security needs) - Presentation

David Owens, Edison Electric Institute (physical infrastructure needs) - Presentation

Jay Apt, Carnegie Mellon University (mitigation and restoration) - Presentation

Sue Tierney, Analysis Group (resilience and critical services)

DOE: A Key Partner in Ensuring a More Resilient and Secure Electric Power Delivery System

Patricia Hoffman, Department of Energy - Presentation

What Is Industry's Role Moving Forward?

Fred Hintermeister, North American Electric Reliability Corporation - Presentation

Cyber Security Needs

Understanding Critical Cyber Vulnerabilities

Panel Discussion

Galen Rasche, Electric Power Research Institute - Presentation

Paul Nielsen, Software Engineering Institute

Terry Boston, PJM Interconnection - Presentation

Open Discussion on Cyber Security of the Grid

Moderated by Massoud Amin, University of Minnesota - Presentation

Thursday, February 28, 2013

Welcome and Introduction

Granger Morgan, Carnegie Mellon University (NRC Panel Chair)

Physical Vulnerability

The Future of the Electric Grid

John Kassakian, Massachusetts Institute of Technology - Presentation

The DHS transformer program

Sarah Mahmood, Department of Homeland Security - Presentation followed by Q&A

Open Discussion on the Physical Vulnerability of the Grid

Moderated by David Owens, Edison Electric Institute

Mitigation and Restoration

Power Disruptions in the United States and Improving Restoration of Service

Panel Discussion

Daniel Bienstock, Columbia University - Presentation

Steve Whitley, NYISO - Presentation

Mike Adibi, IRD Corp. - Presentation

Open Discussion on Mitigation and Response

Moderated by Jay Apt, Carnegie Mellon University

Resilience and Critical Services

Reducing Risk and Increasing National Resilience

Panel Discussion

*Gerry Galloway, University of Maryland (NRC Committee on Disaster Resilience) -
Presentation*

David Kaufman, DHS/Federal Emergency Management Agency

Open Discussion on Resilience

Moderated by Sue Tierney, Analysis Group

What Can We Do to Move Forward?

(Q&A following each speaker)

The Regulatory Environment

Joseph McClelland, Federal Energy Regulatory Commission

How Policy Will Shape Utilities Moving Forward

Miles Keogh, National Association of Regulatory Utility Commissioners

Open Discussion on Policy Options

Moderated by Granger Morgan, Carnegie Mellon University (NRC Panel Chair)

Research and Development Opportunities

Clark Gellings, Electric Power Research Institute - Presentation

Closing Remarks

Granger Morgan, Carnegie Mellon University (NRC Panel Chair)