NATIONAL ACADEMY OF SCIENCES
NATIONAL ACADEMY OF ENGINEERING
INSTITUTE OF MEDICINE
NATIONAL RESEARCH COUNCIL

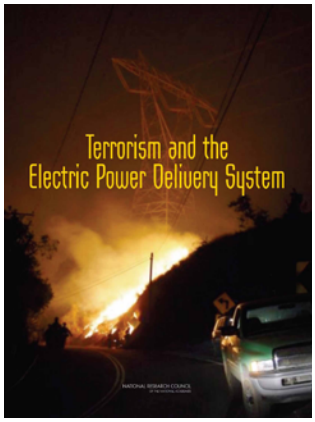
REPORT IN BRIEF

Terrorism and the Electric Power Delivery System

Board on Energy and Environmental Systems • Division on Engineering and Physical Sciences
November 2012

The U.S. power delivery system is remarkably complex. Its network of substations, transmission lines, and distribution lines are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. In addition, investment to strengthen and upgrade the grid has lagged, resulting in a high-voltage system with many heavily stressed parts. Overall, the nation's power grid is in need of expansion and upgrading. Since all parts of the economy—as well as human health and welfare—depend on electricity, the results of a well-planned and coordinated attack on the power delivery system could be particularly devastating. This report[1] examines technologies and strategies that could make the power delivery system less vulnerable to attacks, restore power faster after an attack, and make critical services less vulnerable while the power is out. The approaches explored in the report can greatly reduce the grid's vulnerability to cascading failures, whether initiated by terrorists, nature, or malfunctions.

Vulnerabilities of the Electric Power Delivery System



Today most power is generated by large central generating stations that are located far from the customers they serve. Transformers located near the power plant increase the voltage so that it can be carried efficiently over long distances. Substation transformers near the end user then reduce the voltage and carry the power into the distribution network for delivery to customers. Unlike trains or natural gas in pipelines, electric power cannot simply be sent via specific lines wherever dispatchers choose. The electrical current flows through the system according to a set of physical laws and it must be continually adjusted to keep all parts synchronized and in electrical balance. If corrections are not made immediately when imbalances occur, the result can be oscillations and other disturbances in the system that can result in a cascading failure over a wide area, as happened in the Northeast blackout of 2003.

The system is inherently vulnerable because transmission lines may span hundreds of miles, and many key facilities are unguarded. This vulnerability is exacerbated by the fact that the power grid, most of which was originally designed to meet the needs of individual vertically integrated utilities, is being used to move power between regions to support the needs of competitive markets for power generation.

Recent years have witnessed dramatic organizational changes in the U.S. electric power system. In some states, traditional vertically integrated companies that owned and operated

[1] The full report, *Terrorism and the Electric Power Delivery System*, was completed by a committee of dedicated experts, assembled by the National Research Council (NRC), and delivered to the study's sponsor, the Department of Homeland Security, for security review in 2007. The report being released publicly is an unclassified version. A workshop is being organized for early 2013 to address changes that have occurred affecting the nation's power grid since the report's completion.

the entire system from the generators to the customers' meters have been restructured in an effort to introduce competition. The introduction of competition in bulk power across the country has resulted in the transmission network being used in ways for which it was not designed. Largely as a consequence of the uncertainties introduced by these changes, incentives for investment by private firms have become mixed.

As a result, the physical capabilities of much of the transmission network have not kept pace with the increasing burden that is being placed on it—subsequently many parts of the bulk high-voltage system are heavily stressed. In addition, many important pieces of equipment are decades old and lack improved technology that could help limit outages. This makes the stressed, aging system especially vulnerable to the multiple failures that might follow, for example, a coordinated attack on the power system by terrorists.

If carried out in a carefully planned way, by people who knew what they were doing, such an attack could deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold. Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, at the time of this study international terrorists had shown limited interest in physically attacking the U.S. power grid. However, that should not be a basis for complacency.

Physical Vulnerability

Disruption in the supply of electric power can result from problems in any part of the system, including some transmission lines where the destruction of a small number of towers could bring down many kilometers of line. The large high-voltage transformers are particularly vulnerable to attack both from within and from outside the substation where they are located. These transformers are custom-built, very large, and difficult to move. Large transformers are no longer made in the United States, and the delivery time for new ones can run to months or years. The industry has made some progress toward building an inventory of spares, but these efforts could be overwhelmed by a large attack.

Cyber Vulnerability

Modern power systems rely heavily on automation, centralized control of equipment, and high-speed communications. The most critical systems are the supervisory control and data acquisition (SCADA) systems that gather real-time measurements from substations and send out control signals to equipment, such as circuit breakers. The many other control systems, such as substation automation or protection systems, can each only control local equipment. All SCADA systems are potentially vulnerable to cyber attacks, whether through Internet connections or by direct penetration at remote sites. Any telecommunication link that is even partially outside the control of the system operators is a potentially insecure pathway into operations and a threat to the grid. Wireless communications within substations is a particular concern.

If they could gain access, hackers could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems. Cyber attacks are unlikely to cause extended outages, but if well coordinated they could magnify the damage of a physical attack. For example, a cascading outage would be aggravated if operators did not get the information to learn that it had started, or if protective devices were disabled. Cyber security is best when interconnections with the outside world are eliminated. When interconnections are unavoidable, best practices for security must apply.

Personnel Vulnerability

Workforce issues are critically important to maintaining a reliable supply of electricity, particularly in the event of a terrorist attack. Utility employees and contractors interact with the electric power system as managers, operators, line-crews, suppliers of materials and services, and users. Although workers and managers in this industry have an outstanding record of reliable performance, even a few pernicious people in the wrong place are a potential source of vulnerability.

A second issue is that, to a greater extent than in most other industries, the electricity workforce is aging, and many skilled workers and expert engineers will soon

retire. As the current workforce retires, utilities may have increasing difficulty hiring sufficient numbers of qualified replacements to keep the system operating effectively and reliably and to undertake all the upgrades that are needed, let alone cope with damage from terrorist attacks. This issue requires sustained and high-level attention by both the industry and federal agencies.

Addressing Vulnerabilities: Resilience, Restoration, and Maintaining Critical Services

Many of the changes discussed in this report could convert an attack that today could cause a blackout over a wide region of the country into one that would do less damage to the electric system and leave the system in a better position to accommodate the damage that does occur. Cascading failures could be limited, and many areas within a blacked-out region could maintain power because they could isolate themselves from the failing grid and maintain a balance of generation and demand within their borders. The extent of the damage from an attack can be limited by a variety of means, including improving the robustness of the system to withstand normal failures; adding physical and cyber protections to key parts of the system; and designing it to degrade gracefully after catastrophic damage, leaving as many areas as possible still with power.

After an attack, an electric utility's main focus will be on restoring power to its customers. Many of the next steps would be similar to those taken in response to a major natural disaster, such as a hurricane—that is, identify the damage, clean it up, repair equipment, and restore power. Unlike hurricanes, however, terrorists may strike with no warning and selectively destroy the most important facilities, such as major substations. Some of the lost equipment may take months or even years to replace. A promising solution is to develop, manufacture, and stockpile a family of universal recovery transformers that would be smaller and easier to move.

Physical protection of critical facilities would include hardened enclosures for key transformers, improved electronic surveillance, and system tools that can identify physical and control system problems and potential incidents. Such measures may deter as well as blunt an attack. The risk of insider-assisted attacks can be reduced by strengthening background checks for new and existing employees and contractors. If subversive or disaffected workers can be identified, attackers will lose a major potential advantage. Training operators and other workers to recognize and react to attacks or other major disruptions will be helpful in limiting the extent of outages and further damage during a cascading failure. System simulators are likely to be very useful in this endeavor.

While system owners and operators should do all that they reasonably can to ensure that their systems are able to withstand anticipated assaults from natural and human sources, there are practical limits to how much these highly distributed systems can be hardened. Since the complete elimination of all possible modes of failure is simply not feasible, an important design objective—in addition to resilience and the ability to rapidly restore the system after a problem occurs—should be the ability to sustain critical social services while an outage persists. Thus, in addition to strengthening the grid, federal, state, and local governments should also focus on identifying critical services and developing strategies to keep them operating in the event of power outages, whether accidental or the result of terrorist attack.

There are many technologies and strategies that could be employed to make the power system more robust in the face of a terrorist attack, make service restoration more timely after an attack, and continue the provision of critical services while the power is out. The best way to make these needed changes affordable—and to develop new, even more effective and affordable approaches—is through research. For the most part, this is the same research that would also address the broad problems faced by the aging transmission and distribution grid. In the long term, supporting engineering and other technical education will help to maintain the availability of the necessary skills in the workforce as well.

Overall, the level of protection for and resiliency of the electric power grid against terrorist attacks needs to increase. However, the level of security that is economically rational for most infrastructure operators will be less than the level that is optimal from the perspective of the collective national interest. Therefore, the DHS should develop a coherent plan to address the incremental cost of upgrading and protecting critical infrastructure to that higher level.

Background on this Report

The full *Terrorism and the Electric Power Delivery System* report was prepared by a committee of dedicated experts, assembled by the National Research Council (NRC). As required under contract, the report was submitted to the sponsor, the Science and Technology Directorate of the Department of Homeland Security (DHS), for security classification review in the fall of 2007. In August 2008, DHS concluded that the report would be classified in its entirety. Because the committee believed that the report as submitted contained no restricted information, the NRC requested the formal classification guidance constituting the basis for the classification decision. Finally, in August 2012, the current full report was approved for public release—reversing the original classification decision, except that several pages of information deemed classified are available only to readers with the necessary security clearance.

Even though the committee's work was completed in 2007, the report's key findings remain highly relevant. Major cascading blackouts in the U.S. Southwest in 2011, and in India in 2012, underscore the need for the measures discussed in this report. In fact the report already has helped DHS focus on research aimed at developing a recovery transformer that could be deployed rapidly if many large power transformers were destroyed. Electric utilities and other private sector entities, state and local governments, and others involved with electric power are also likely to find the information in this report very useful. Nonetheless, since the report was completed in 2007, concurrent with the report's release to the public, a workshop is being planned for early 2013 to address changes that have occurred since the report's completion in 2007. The workshop "The Next Generation Power Grid: Security, Reliability, and Efficiency" will also assess the current state of electric power transmission and distribution in the United States and explore important considerations for the future.

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack: M. Granger Morgan, Carnegie Mellon University, Chair; **Massoud Amin,** University of Minnesota; **Edward V. Badolato,** Integrated Infrastructure Analytics Inc. (deceased as of 2008); **William O. Ball,** Southern Company Services; **Anjan Bose,** Washington State University; **Clark W. Gellings,** Electric Power Research Institute; **Michehl R. Gent,** North American Electric Reliability Corporation (retired); **Diane Munns,** Edison Electric Institute; **Sharon L. Nelsom,** State of Washington Attorney General's Office (retired); **David K. Owens,** Edison Electric Institute; **Louis L. Rana,** Consolidated Edison Company of New York; **B. Don Russell Jr.,** Texas A&M University; **Richard E. Schuler,** Cornell University; **Philip R. Sharp,** Resources for the Future; **Carson W. Taylor,** Bonneville Power Administration (retired); **Susan F. Tierney,** Analysis Group; **Vijay Vittal,** Arizona State University; **Paul C. Whitstock,** Marsh USA Inc.

Project Staff

Board on Energy and Environmental Systems: Alan Crane, Study Director; **Duncan Brown,** Senior Program Officer (until July 2010); **Harrison T. Pannella,** Senior Program Officer (until July 2007); **James J. Zucchetto,** Director, BEES

National Academy of Engineering Program Office: Penelope Gibbs, Senior Program Associate; **Jack Fritz,** Senior Program Officer (until 2006)

This study was supported by a contract between the National Academy of Sciences and the U.S. Department of Homeland Security. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

Copies of this report are available free of charge from http://www.nap.edu.

Report issued November 2012. Permission granted to reproduce this brief in its entirety with no additions or alterations. Permission for images/figures must be obtained from their original source.

© 2012 The National Academy of Sciences