
# SECURING THE U.S. ELECTRICAL GRID

THE HONORABLE THOMAS F. McLARTY III
&
THE HONORABLE THOMAS J. RIDGE
*PROJECT CO-CHAIRS*

CSPC

The Center for the Study of the Presidency and Congress, founded in 1965, is a nonprofit, nonpartisan 501(c)(3) organization. The Center's mission is to utilize the lessons of history to address the challenges of today; serve as a strategic honest broker for discussions with leaders from government, the private sector, and the policy community; and to educate the next generation of leaders through the Presidential and International Fellows Program.

SECURING THE U.S. ELECTRICAL GRID



Published in the United States of America.

Cover Photo Credits: iStock by Getty Images (main, top right); U.S. Department of Energy (top left, top center)
Icon Templates by www.visualpharm.com


CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

1020 Nineteenth Street, NW, Suite 250
Washington, D.C. 20036
Phone: 202-872-9800
Fax: 202-872-9811
www.thePresidency.org


CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

# SECURING THE U.S. ELECTRICAL GRID

## UNDERSTANDING THE THREATS TO THE MOST CRITICAL OF CRITICAL INFRASTRUCTURE, WHILE SECURING A CHANGING GRID

***PROJECT CHAIRS***

THE HONORABLE
THOMAS F. McLARTY III

THE HONORABLE
THOMAS J. RIDGE

***PROJECT DIRECTORS***

MAXMILLIAN ANGERHOLZER III
FRANK J. CILLUFFO
DAN MAHAFFEE

***LEAD RESEARCHER***

MADELINE VALE

***EXTERNAL AFFAIRS***

JONATHAN MURPHY

WASHINGTON, D.C.
OCTOBER 2014

# TABLE OF CONTENTS

# ACKNOWLEDGEMENTS

On behalf of the Center for the Study of the Presidency & Congress, I want to thank the following for their contributions to the project, "Securing the U.S. Electrical Grid":

The Smith Richardson Foundation, whose generosity allowed the Center to embark on a yearlong effort to study ways in which the U.S. can better secure its electrical grid. This project included eight off-the-record sessions on the East and West Coasts, as well as countless meetings with both public and private sector leaders.

Dr. David M. Abshire, Vice Chairman & President *Emeritus* of the Center, who continues to be the driving force behind the Center's efforts to strengthen our nation's security and bridge the divide between the public and private sectors.

Ambassador Mack McLarty and Governor Tom Ridge, who not only serve as CSPC Trustees, but also co-chairs of this effort. Their advice, guidance, and leadership throughout the project were invaluable.

Senator Chuck Hagel, former CSPC Trustee, who co-chaired our original cybersecurity project—which helped lay the groundwork for this effort—before answering President Obama's call to become Secretary of Defense.

My fellow Project Directors, Frank Cilluffo, who is a Senior Fellow at CSPC, and Dan Mahaffee, the Director of Policy & Board Relations at CSPC. Without their tireless work and seemingly never-ending energy and enthusiasm for the project we would not have arrived where we have today.

Jonathan Murphy, CSPC Director of External Affairs, who did an excellent job convening leaders from public and private sectors across the county to take part in this effort.

Madeline Vale, who served as Lead Researcher for the project, deserves thanks for the countless hours and extremely hard work dedicated to coordinating this effort.

Our entire team at the Center, including, Marili Alvarado, Andrew Crum, Summer Fields, Rachel Johnson, Natalia Kapani, Willy Nash, Ann Marie Packo, Elizabeth Perch, Nicholas Platt, Grace Priest, Hurst Renner, Sara Spancake, Ben Stutts, Parker Toms, Alexandra White, Ghazal Zafar, and Melanie Zook.

Finally, I would like to thank all those who participated in the roundtables and meetings, giving us invaluable advice and perspective.

Maxmillian Angerholzer III
President & CEO
Center for the Study of the Presidency & Congress

# PREFACE

Following the end of World War II, the Allied Strategic Bombing Survey—responsible for determining the damage inflicted by U.S. and Allied strategic bombing of German and Japanese industry—determined that the bombing campaign would have been more effective if it had targeted the German and Japanese electrical grid rather than urban and industrial centers.

More than seventy years later, the secure and reliable delivery of electricity is a vital cornerstone of modern American society. For those who would seek to do our Nation significant physical, economic, and psychological harm, the electrical grid is an obvious target. In addition to malicious actors, the grid regularly faces the challenge of extreme weather events that affect wide swaths of the United States.

The electrical grid is currently undergoing rapid change with the development of Smart Grid and microgrid technologies, as well as the increased use of renewable generation and distributed generation. As the grid moves from the "Edison Era" to the "Google Era," there is an opportunity to build a more secure, more resilient, and more efficient grid. At the same time, it is worth recognizing what utilities have already accomplished in planning for the complexities of these new systems and the implications of deterring new and advanced threats.

In a future where electric cars may connect to a Smart Grid and transfer unused electricity back into the grid, securing the grid will require the attention not only of utility companies, but also of consumers and the manufacturers of the car and its components and this complexity is just one of the examples raised in discussing the future of the grid.

Mitigating these threats, overcoming these challenges, and harnessing these opportunities all require coordination and cooperation between the White House, executive branch agencies, Congress, the utility industry, other private sector entities, and the American people. As new threats arise, we must adapt to face them. As new innovations are implemented, we must adjust how we use carrots and sticks to meet standards and encourage best practices.

As an organization focused on applying the lessons of history to the challenges of today, the Center for the Study of the Presidency & Congress has utilized the model of some of our nation's greatest modern Presidents—FDR, Eisenhower, Kennedy, and

Reagan—by bringing together the best and brightest from across multiple sectors of government, business, and society to deliberate and share ideas on this issue.

This project has sought to address these challenges and begin a new conversation about the security of a changing grid. Through off-the-record roundtable discussions with experts from government, the private sector, and the policy community, this project has examined the threats of cyberattack, physical attack, electromagnetic pulse, and severe weather. We have explored how the executive branch organizes itself to address the security of critical infrastructure—focusing on the grid. We have analyzed the path of legislation related to grid security and the political obstacles it faces. We have discussed how the private sector can better support and incentivize best practices and innovations for security and reliability. We have looked at what the future of the grid may hold in terms of both new technology and a shift to renewable energy.

From this process we have assembled these twelve key recommendations and the broader report on the security of the grid and its future. We feel that we have developed pragmatic, realistic findings to be utilized by policymakers, utility executives, and informed citizens.

This discussion will continue to evolve and this report will be a jumping-off point—both for our continued efforts and those of others.

We hope that this report and these findings provide the tools to ensure that the lights are always on.


Maxmillian Angerholzer III
Project Co-Director
President & CEO
Center for the Study of the Presidency & Congress

Frank J. Cilluffo
Project Co-Director
Senior Fellow
Center for the Study of the Presidency & Congress

Dan Mahaffee
Project Co-Director
Director of Policy & Board Relations
Center for the Study of the Presidency & Congress

# LIST OF ROUNDTABLES

*The Electrical Grid: Political & Regulatory Dynamics*
September 30, 2013
Washington, D.C.

*Federal Agencies & Utility Operators*
November 5, 2013
Washington, D.C.

*Political Dynamics Surrounding Cybersecurity Legislation & Electrical Grid Solutions*
December 16, 2013
Washington, D.C.

*Physical Threats: Terrorism, Vandalism & Weather*
February 21, 2014
New York, New York

*Investment in Strengthening & Modernization*
March 25, 2014
Los Angeles, California

*Cyber Vulnerabilities & Security Technology*
March 27, 2014
San Francisco, California

*Electromagnetic Pulse, Geomagnetic Storm & Directed Energy*
May 5, 2014
Washington, D.C.

*Project Findings & The Path Forward*
June 9, 2014
Washington, D.C.

# SUMMARY OF FINDINGS

## OVERALL FINDINGS

**#1: The case for electrical grid security must be built through a comprehensive, strategic, risk-based approach.** The grid faces a multitude of threats and vulnerabilities—cyberattack, physical attack, electromagnetic pulse (EMP), geomagnetic storm, and inclement weather—from a multitude of actors. Focusing on one event or one type of attack fails to account for the overlapping nature of many of these threats. However, with finite resources, if we attempt to address all threats and vulnerabilities, we protect against none. Using a comprehensive, risk-based approach, grid security can be addressed in a manner that balances protection with the need to provide affordable energy to consumers.

## SHORT-TERM

**#2: The Obama Administration should continue to pursue actions that facilitate grid security and critical infrastructure security.** Recent actions by the Administration—the Executive Order 13636 on cybersecurity and critical infrastructure; the National Institute of Standards and Technology (NIST) framework for cybersecurity; and the Department of Justice–Federal Trade Commission (DOJ-FTC) statement that information sharing regarding cybersecurity does not constitute anticompetitive behavior—have been significant steps towards improving grid security. The Administration should take further steps to aid information sharing within government and industry, and between the two. This includes: that the Federal Communications Commission (FCC) ensures that utility operators have access to spectrum and communications necessary for information sharing and service restoration during an incident; steps to ensure that the information shared with industry is both timely and useful; and further discussions of Executive and Legislative action aimed at allaying concerns about liability and privacy protection.

**#3: Congress must act to codify structures for cybersecurity information sharing.** While the Administration has done much to advance information sharing using Executive powers, only the Congress can provide the legal frameworks that address concerns about liability and privacy protection. The leadership in Congress must act to resolve the deadlock that has stymied legislation aimed at addressing cybersecurity information sharing and critical infrastructure protection.

**#4: Exchange programs should be developed to allow government employees to temporarily work at private sector utility companies and vice versa.** Ultimately, trust cannot be legislated. Building relationships between government officials handling security information and utility officials responsible for security can improve the knowledge base and communication procedures regarding grid security issues.

**#5: Where possible, security information sharing should be an automated process.** Already, the government and industry are using pilot programs—such as the Cybersecurity Risk Information Sharing Program (CRISP) and the Trusted Automated eXchange of Indicator Information (TAXII)—that allow for immediate sharing of security information. Machine-to-machine information sharing will allow for the most rapid response to potential threats, as it can promptly share information that has cleared the "tear line" process and has been anonymized to protect privacy information.

**#6: The business model for further electrical grid security investments must also include private sector actors, such as the insurance industry and the financial sector.** Arguably one of the most heavily regulated industries, utility operators already meet a bevy of standards set by federal, state, and industry bodies. The insurance underwriting process provides a key opportunity to analyze and model the risks a utility faces, as well as the incentives—through premiums and other tools—for adopting best security practices.

## LONG-TERM

**#7: The Department of Energy should continue its role as the "Sector-Specific Agency" for electrical grid security.** As the "Sector-Specific Agency" for the Energy Sector, the Department of Energy works with the utility industry to address grid security issues. Continuing to keep direct regulatory oversight separate from security discussions is the best arrangement for fostering dialogue and information sharing regarding grid security. The Department of Homeland Security should continue its role as the lead agency on broader critical infrastructure protection and cybersecurity, alongside its ongoing work with the Intelligence Community on threats originating from overseas, and law-enforcement domestically.

**#8: Grid security must be better understood in conjunction with the other critical infrastructures and supply chain on which the grid relies.** Secure, reliable electrical grid operations rely on various other critical infrastructures—water, gas, and telecom, to name a few. The Department of Homeland Security should continue to work with the sector-specific Information Sharing and Analysis Centers to ensure that grid security also includes the security of ancillary critical infrastructures and a resilient supply chain.

**#9: Congress must explore options to better coordinate grid oversight and grid-related legislation.** While the U.S. House Committee on Energy & Commerce and the U.S. Senate Committee on Energy & Natural Resources have immediate jurisdiction over electrical grid issues, the Committees on Homeland Security, Intelligence, and the Armed Services also play significant roles in the security of the grid and other critical infrastructure. Congressional Leadership, the chairs, and ranking members of these committees should work together for better legislation and oversight in these areas. Inter-committee coordination can be facilitated through ongoing staff work, and the leadership of these committees should consider joint public events as a tool for raising awareness—among both Members of Congress and the public—about grid security.

**#10: Government and the utility industry should seek to build Public-Private Partnerships (PPPs) for improved grid resilience and security.** Combining the resources of the private sector, the technical know-how of national labs and technology companies, and the capabilities of government can provide innovative solutions for grid security. Government and industry partnership can address areas such as replacement transformer reserves, warehousing and prepositioning of resources, and other logistical support. In addition, through this preparation process, these relationships can facilitate the planning for the response to and recovery from a catastrophic event.

**#11: State resources, especially the National Guard, should be integrated into grid security planning.** Some states, notably California and Michigan, have developed structures that formally involve state utility regulators and state emergency management agencies in incident response plans. With the support of the state National Guard, these states have developed security auditing and reserve capabilities that can address grid security incidents. As part of this process, National Guard units and other state agencies should increase the number of "red-team exercises" and other preparatory measures. Where appropriate, state authorities should also be included in national exercises such as "GridEx."

**#12: Unresolved questions about the implementation of Smart Grid, microgrid, and the shift to renewable generation require further examination with an eye towards grid security and reliability.** Advanced technologies have the potential to improve the security of the grid, while also addressing concerns about climate change and environmental impact. However, the implementation of these technologies has the potential to greatly disrupt the economic and commercial structures for electricity generation and distribution, and thus concerns about the business model for providing a secure and reliable electric supply.

# EXECUTIVE SUMMARY

## OVERVIEW

Arguably the most critical of critical infrastructure, the U.S. electrical grid is the backbone of our modern society. Vital sectors such as the financial industry, transportation, telecommunications, public safety, and other utilities rely on electricity for their operations. In turn, the grid itself is reliant on the infrastructures and supply chains that support its operations—such as water, oil and gas, and telecommunications.

An obvious target to a range of actors who would seek to strike at the U.S. homeland, the grid also faces significant security challenges due to not only increased demand, but also the challenge of modernizing outdated infrastructure with new technologies and control systems.

While this modernization entails significant challenges in its own right, it also provides an opportunity to "bake security in"—both in the hardware and software controlling these systems and in the business models, regulatory systems, financial incentives, and insurance structures that govern the generation, transmission, and distribution of electric power.

First and foremost, grid security is based on the protection of the grid from physical attack, cyberattack, inclement weather, electromagnetic pulse, and geomagnetic storm, as well as the ability to mitigate and recover from such an event quickly. This combination of intelligence, early warning, strength, and resilience serves as a deterrent factor in its own right.

Still, if we seek to protect everything, we will protect nothing. Risk-based analysis—combined with an understanding of critical facilities, key network nodes, and vital control systems and ancillary infrastructure—allows for the best use of limited resources.

In this report and the aforementioned dozen recommendations, we have sought to identify the immediate action that can be taken by the White House, the Congress, and the private sector to mitigate current threats to the electrical grid.

A unique dynamic now exists, as private sector utility providers find themselves on the front lines of national security issues that were once the sole responsibility of nation-states. In some areas, immediate action can be taken by the Obama Administration.

One example is actions that promote information sharing about threats to grid security in a manner that is rapid, while also allowing for the protection of private information. Another is the development of personnel exchanges between the utility industry and government agencies responsible for grid security or regulation.

In other areas, legislative action—at the federal and state levels—is needed to address these concerns. Key areas that need legislative action include the creation of formal mechanisms for rapid information sharing regarding physical and cyber threat information between the private sector, sector specific agencies, and the intelligence community. Furthermore, only legislation can address issues of privacy protection, liability protection, and other concerns raised by utility operators.

Other solutions—including incentives for new security measures and practices—can come from the financial and insurance industries. For example, the insurance underwriting process can serve as an opportunity to evaluate vulnerabilities, share information about threats, and encourage best practices for risk mitigation. Still, further examination will be needed to understand how to best price the risk of novel threats, such as cyberattack and the value of investments and public-private partnerships in modernizing grid infrastructure.

In the long run, the security of the grid will also depend on how we incorporate new technology into aging infrastructure. Some of these technologies allow for the increased use of cleaner or fully renewable generation sources and allow for the move to more resilient "microgrids" with distributed generation. However, while more resilient, such Smart Grid and microgrid systems present significant challenges to grid security.

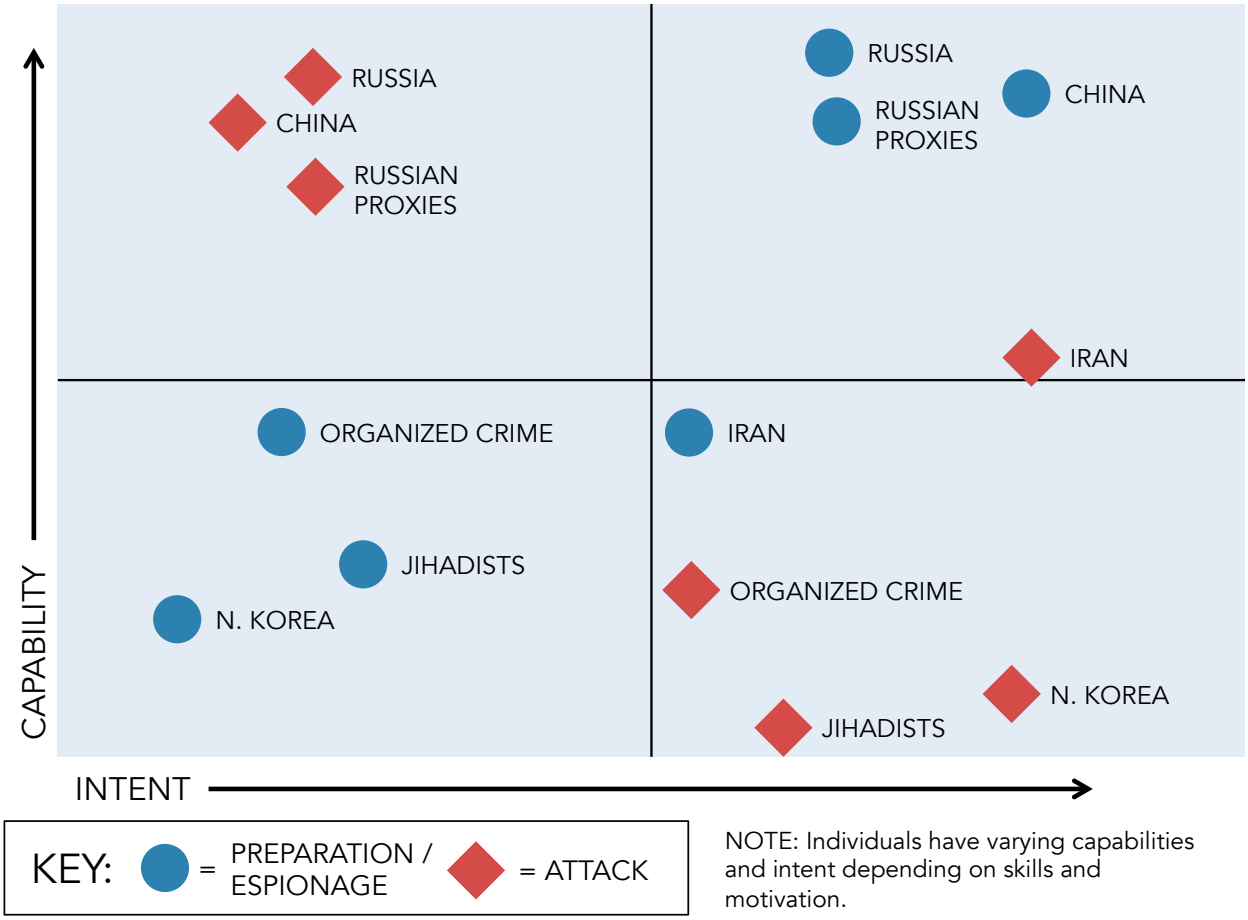
First, as Smart Grid and microgrid technologies become more common, the physical and cyber access points to the grid will increase exponentially. As a broader array of devices, appliances, and systems connect to the grid and networked control systems, an increased number of manufacturers and users become involved in standards for grid security.

Second, with the deployment of distributed generation systems and microgrids, there is a likely disruption to traditional utility business models based around centralized generation and the national distribution of bulk electric power. These business models allow for the cost recovery necessary for improvements in security and infrastructure. As these technologies are developed, new business models must also be explored—ones that incorporate insurance incentives, public-private investments, net metering, and other advances.

Finally, as the United States shifts towards renewable sources of generation, grid security will also involve a balanced portfolio of energy sources that harnesses our nation's natural resources and technological innovations. In examining some of the lessons of the German energy transition, it is important for the United States to responsibly balance environmental needs, existing resources, and political decision-making.

Through responsible, pragmatic policies, the United States can build a cleaner, more efficient electrical grid, while also ensuring that consumers and companies have reliable, affordable electricity.

## INTENTS & CAPABILITY OF THREAT ACTORS

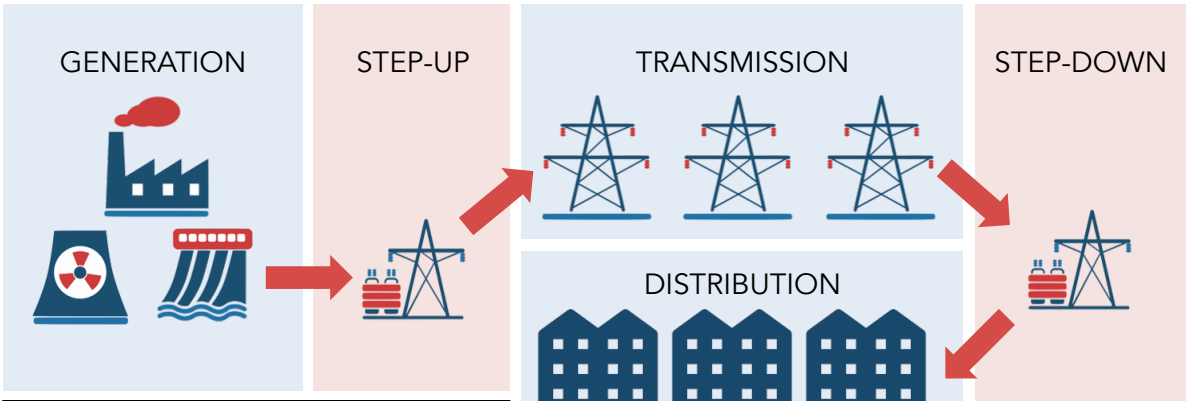



KEY: ● = PREPARATION / ESPIONAGE ◆ = ATTACK

NOTE: Individuals have varying capabilities and intent depending on skills and motivation.

## PRESENT & FUTURE MODELS FOR THE GRID

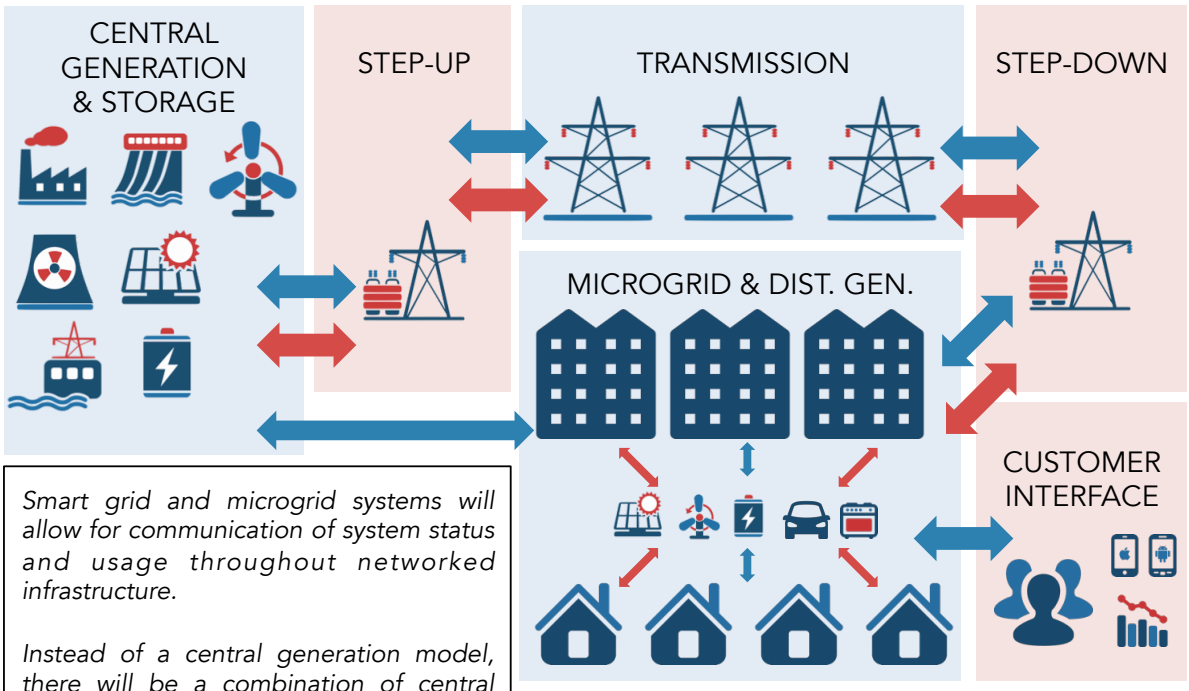
### PRESENT MODEL




*Centrally-generated power flows from generation plants through the bulk power system to industrial, commercial, and residential users.*

KEY: = POWER = DATA

### FUTURE MODEL




*Smart grid and microgrid systems will allow for communication of system status and usage throughout networked infrastructure.*

*Instead of a central generation model, there will be a combination of central generation, storage of renewable energy from peak generation, and distributed generation from renewable sources and cogeneration.*

# UNDERSTANDING THE THREATS

## CYBERATTACK

Paradoxically, as the grid is increasingly networked—thus increasing efficiency and overall situational awareness—it becomes increasingly vulnerable to intrusions from cyberspace. Older grid systems are likely to have "air gaps" between the public Internet and SCADA or other control systems. However, as Smart Grid technologies are installed, there will be a greater number of access points to the grid networks, requiring increased security awareness by utilities, device manufacturers, and the general public. Still as many of these products are still being designed and deployed, there is an opportunity to "bake security in" to software and hardware systems under development.

A wide range of actors have sought to exploit cyber vulnerabilities in the U.S. electrical grid. On one hand, nation-states like Russia, China, Iran, and North Korea look for vulnerabilities that would allow them to strike at the U.S. homeland. On the other, non-state actors including foreign terrorist groups, ecoterrorist groups, and organized crime networks seek vulnerabilities for both violence and profit, such as blackmail or extortion. Individuals may hack grid networks out of curiosity or to raise their profile within hacking communities.

Ultimately, not all cyber intrusions, cyber espionage, and/or cyberattacks are the same. While attribution within the cyber domain remains challenging, understanding the purpose of the assailant better informs the security response—e.g. cyber espionage of technology versus preparation for cyberattack.

## PHYSICAL ATTACK

Physical attack can take many differing forms. Recent events examined during the course of the project included the highly complex attack on the Metcalf Substation in California and the vandalism of transmission lines and facilities in Arkansas. Due to the diffuse nature of the grid, securing the entire system against physical attack is challenging. Still, the networked nature of the grid and increasing connectivity through Smart Grid technology allows for better security and resiliency.

Defending against physical attack requires ongoing intelligence gathering of potential threats; improved surveillance and hardening of key facilities; drilling and preparation in advance of any incident; and the ability to quickly mitigate the effects of any attack and quickly restore service. Of significant importance to recovery from physical attack is the ability to quickly repair or replace damaged equipment.

Attacks targeting transformers are an area of particular concern, as there are difficulties due to their cost, size, and complexity, as well as the fact that some transformers are custom-built for the facility in which they operate. As the utility industry has begun to stockpile replacement transformers, the security of the stockpile's warehouses and facilities and the ability to transport replacements to where they are needed also becomes a concern.

Given that a major cyberattack on grid infrastructure would require significant resources in terms of intelligence gathering and hacking expertise—nation-state level resources—a physical attack will be the likely method for smaller non-state actors and individuals seeking to cause grid disruption. In addition, electrical utilities also must harden the grid against a joint physical and cyberattack—or the consequences of a cyberattack that causes physical damage to grid equipment.

## ELECTROMAGNETIC PULSE

Caused by the high-altitude detonation of a nuclear weapon, electromagnetic pulse (EMP) can cause widespread damage to electric systems across a wide area. While this is a significant threat to grid security, there are a limited number of actors that could execute such an attack, and such an attack would be a direct act of war. Furthermore, since high-altitude nuclear tests were banned by treaty in 1963, there is only limited scientific data about the impact of such a nuclear detonation on modern infrastructure.

Still, given the potential damage that an adversary could cause through EMP, both the government and the utility industry should work together to identify measures that could mitigate the effect of an EMP and rapidly restore power to key military, government, and civil facilities. Hardening key grid nodes, microgrid technology, and generation capacity at key facilities are initial measures that could be taken to address vulnerabilities to an EMP attack.

## DIRECTED ENERGY WEAPONS

Directed energy weapons (DEWs) use highly focused energy to create destructive effects across the electromagnetic spectrum—radio waves, visible light, or infrared heat. DEWs that could produce effects similar to an EMP are of particular concern for electrical grid security, because they do not involve the complexity of a missile launch and nuclear detonation. Additionally, DEWs allow an adversary to target specific facilities rather than a wide swath of territory, making their use a far less escalatory option.

While many DEWs are in the development stages and many details remain classified, other nations, particularly China, have placed an emphasis on their development and fielding. Similar to EMP, mitigating a potential DEW strike involves a combination of hardening key nodes and improving grid response and resiliency.

## GEOMAGNETICALLY-INDUCED CURRENTS

Caused by severe solar storms and a coronal mass ejection (CME), a geomagnetically-induced current (GIC) is caused by variations in Earth's magnetic field that produce currents in transmission lines that can damage transformers and other electrical equipment. The largest known event, the "Carrington Event" of 1859, had worldwide implications for telegraphic communications. Smaller events are known to affect infrastructure at higher latitudes. Given the exponentially increased reliance on electricity and telecommunications compared to 1859, a major GIC from a solar storm could have a severe impact on both grid security and society as a whole.

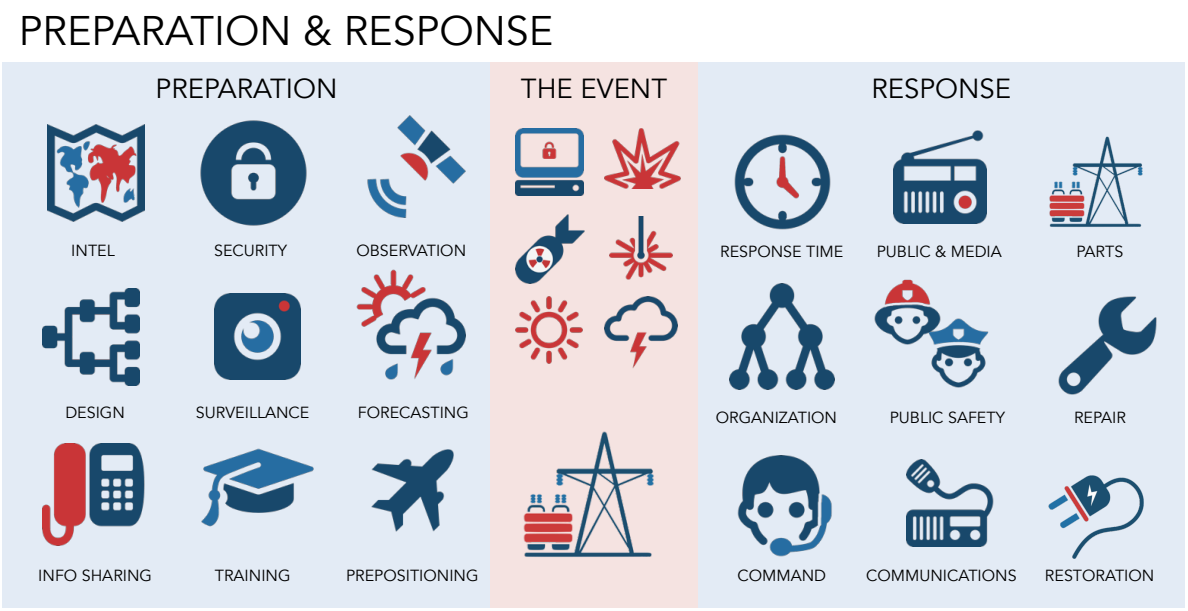
Mitigation strategies for a GIC are similar to that of EMP, but there is increased warning time through ongoing solar observation by space-based and land-based platforms. With a lead-time of two to three days, utility operators would have the opportunity to protect key systems in advance of the CME affecting Earth's magnetic field. Further steps for mitigating GIC include continued support for solar observatory programs; increased scientific research into solar activity and GICs; and continued communication between NASA, NOAA, and the utility industry.

## SEVERE WEATHER

Severe weather is one of the most common causes of damage to the electrical grid, and significant events like the 2012 Derecho, Superstorm Sandy, and other incidents illustrate the effects of high winds, flooding, extreme heat, drought, and earthquake. A combination of aging infrastructure, increased population in vulnerable areas, and climate change has increased the likelihood of damaging weather events. However, given the frequency of these events, the utility industry has significant experience in both preparation for and response to severe weather.

Improved weather prediction capabilities and coordination with federal, state, and local authorities can bolster existing utility industry tools—such as mutual assistance agreements—for responding to severe weather. Smart grid and microgrid innovations can also improve grid resilience and speed power restoration. Finally, the models and capabilities developed for response to severe weather can serve as lessons for preparation and response to some of the aforementioned threats to grid security.

## TOOLS FOR PREPARATION & RESPONSE



# EXECUTIVE ACTION

*The Obama Administration has been actively engaged in the issue of grid security and critical infrastructure protection. In an environment of ongoing political deadlock, the Executive Branch can pursue alternative pathways involving Executive Orders and other measures short of legislation, while still working with Congress.*

EXECUTIVE ORDER 13636, PPD-21 & THE NIST FRAMEWORK
- Expand liability protections and avenues for information sharing
- Add nuance to what may be seen as "one-size-fits-all" standards
- Expedite needed clearances for classified security information
- Work with industry on implementation

VARIED AUTHORITIES FOR GRID SECURITY
- Continue role of Department of Energy as sector specific agency
- Use QHSR process to evaluate and improve DHS role with ISACs and information sharing with state and local authorities, as well as exchange with intelligence agencies

LIABILITY CONCERNS & INFORMATION SHARING
- Build on joint DOJ-FTC announcement regarding cyber threat information and anticompetitive behavior
- Explore options for industry-created limited liability corporation as avenue for increased information sharing with government

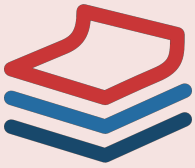
PERSONNEL PROGRAMS
- Provide avenues for exchange of security personnel and management between utility industry and government
- Utilize programs like Scholarship for Service and other incentives for security training and hiring in government agencies

THE ROLE OF NATIONAL LABS
- Build on pilot programs for automated information sharing developed at national labs
- Support research into the effects of EMP, defenses against DEW, and computing systems for automated cybersecurity responses.

LEGISLATIVE AFFAIRS
- Where possible, work with Congress to develop legislation to address grid security issues
- As legislation moves piece-by-piece, bolster gaps in authority with executive orders and other administrative tools

# LEGISLATIVE ACTION

*Thus far, none of the major legislative proposals regarding critical infrastructure protection and cybersecurity have become law. Attempts at comprehensive legislation have met with failure, while piece-by-piece legislation—with a few exceptions—remains in committee. Still, there are key areas of grid security that require Congressional action.*



EXISTING LEGISLATIVE PROPOSALS

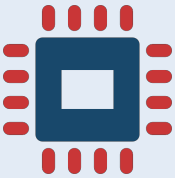
- In varied committees of jurisdiction, legislation that can address grid security has made little progress
- Where bipartisan and bicameral support for proposals exists, Congressional leadership should move these proposals to the floor

LIABILITY & PRIVACY CONCERNS

- Industry executives in multiple sectors, including the electric utility industry have expressed concerns about information sharing liability and the protection of private information
- Only Congress can provide legislation for these issues

COMMITTEES OF JURISDICTION

- Oversight of the electrical grid is split between industry oversight and security oversight
- Leadership of these committees should work together for better oversight and legislation addressing grid security



SUPPLY CHAIN SECURITY

- Where possible Congress should use "the power of the purse" and government buying power to improve supply chain standards
- Legislation can also provide better protections against the importation of counterfeit or otherwise compromised hardware

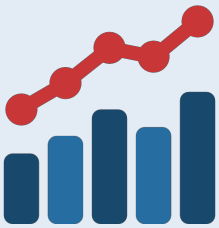
EDUCATION & WORKFORCE

- Legislation-based incentives for cybersecurity and other security careers can ensure that the government and utilities have needed personnel and expertise
- Legislation can also support exchange programs for security experts

RESEARCH & DEVELOPMENT

- Congress should continue to support the mission of the national labs and other research organizations developing grid innovations
- Scientific research in areas such as EMP, solar weather, and other grid security tools can benefit from government grants and support

## INSURANCE & FINANCE



*The insurance industry can play a key role in sharing threat information, mitigating risk, and incentivizing best practices. The underwriting process—combined with active communication between utility and insurer—can ensure ongoing and up-to-date risk evaluation. Other private sector incentives can provide incentives for new technology.*

UNDERWRITING PROCESS & INFORMATION SHARING

- Underwriting process and underwriters' expertise can be used to evaluate vulnerabilities
- Insurance industry can work with utilities to spot security trends
- Best practices can be incentivized through premiums and rates

DATA ANALYSIS

- The insurance industry is harnessing increased connectivity and data collection to analyze and model risk
- Smart grid innovations can provide for real-time information analysis and improve communication between insurer and utility

INNOVATION PARTNERSHIP & INCENTIVES

- Private sector capital can play a significant role in grid innovation and the adoption of new technologies
- Investment in security technologies can be bolstered by public-private cooperation and partnership

## THE FUTURE OF THE GRID

Smart grid technologies will allow for utility operators to have greatly improved situational awareness about grid operations. These systems will improve the resiliency and reliability of the grid, as power can be more quickly rerouted around damaged components, and as utilities can more quickly detect and repair affected portions of the grid.

Smart grid technology will also allow for the connection of many appliances, systems, and tools that previously remained unconnected to the grid. With these innovations, there are significant security challenges as these devices represent a new attack vector for malware or other disruptions. Securing these components will be vital to the health and success of widespread Smart Grid adoption and the use of connected smart appliances.

Microgrid technology—the development of smaller, localized, and self-sufficient grids—represents a key innovation in terms of providing resiliency for the grid, especially when it comes to powering key facilities. An electrical grid made up of multiple microgrids would have the ability to generate power locally, increasing the likelihood of avoiding power interruptions.

Despite this improvement in resilience, there needs to be further examination of the impact that microgrid technology would have on the utility business model that provides for the cost recovery necessary for security and infrastructure improvements, as well as the central generation model that provides both the needed base load for the grid and the long-distance transmission of power needed in a national grid system.

Finally, as the United States seeks to increase efficiency and reduce its carbon footprint, there will be a transition to cleaner fuels—mainly natural gas—and renewable generation sources. The natural gas boom in the United States has greatly lowered the price of domestic natural gas. While this is a benefit for near-term energy prices, it has raised concerns about the long-term viability of capital-intensive investments in new nuclear generation or renewable sources.

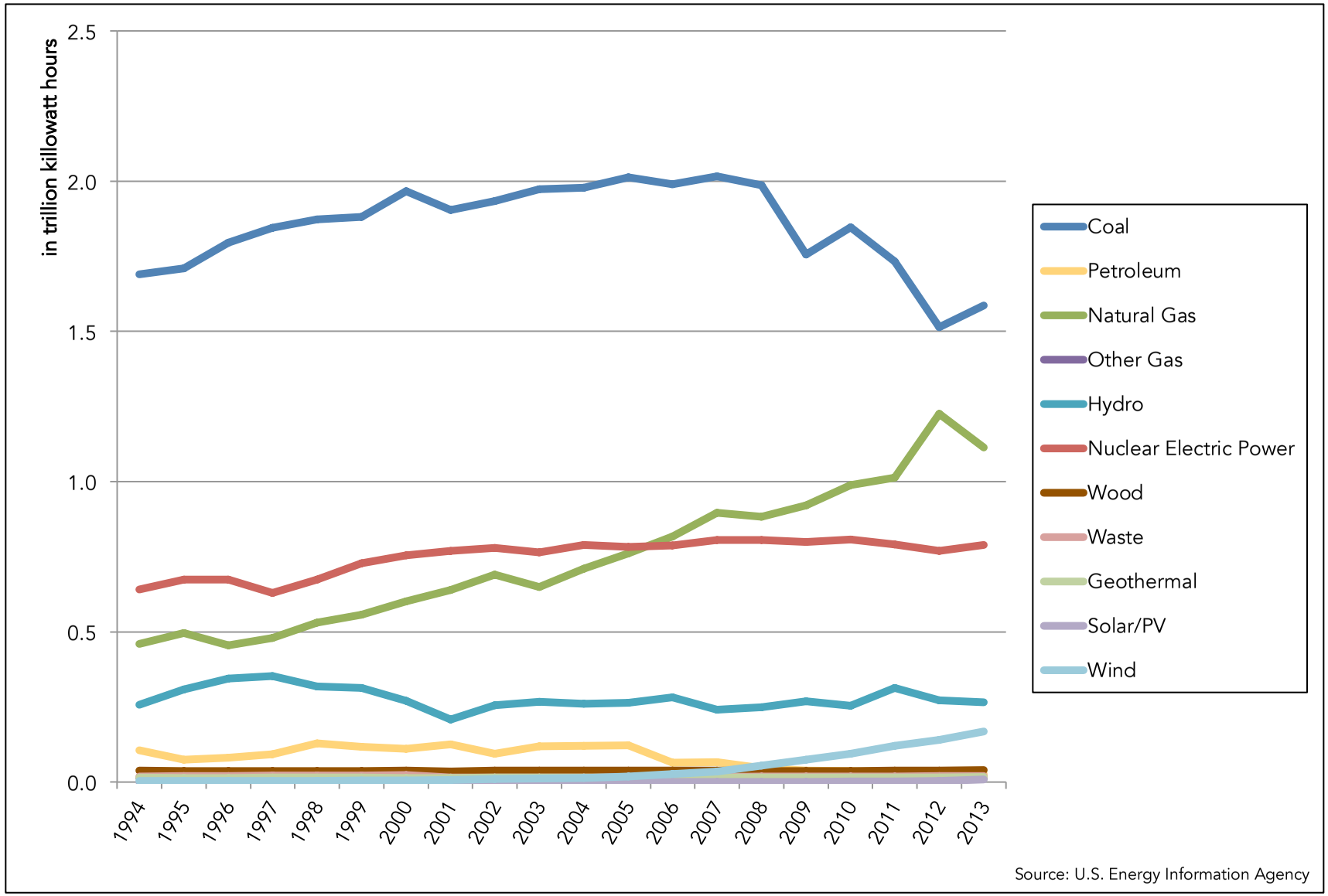
As the chart on the following page shows, these trends have reshaped how the United States gets its electricity, and future policies and market trends will likely further reshape the energy portfolio.

While the United States should continue to harness bountiful natural gas, it is a limited resource, and questions remain about the political environment for nuclear generation and the ability of renewable generation to meet all of our energy needs.

As some nations have completely moved away from nuclear generation, they have found that it has caused significant disruption as it has increased energy prices, and in some circumstances, carbon outputs.

A sound environment and a reliable electricity supply are not mutually exclusive, but policymakers need to examine how the United States shapes its future electrical generation portfolio, to ensure that needed facilities and infrastructure can be developed.

## TRENDS IN GENERATION & RENEWABLES




Source: U.S. Energy Information Agency

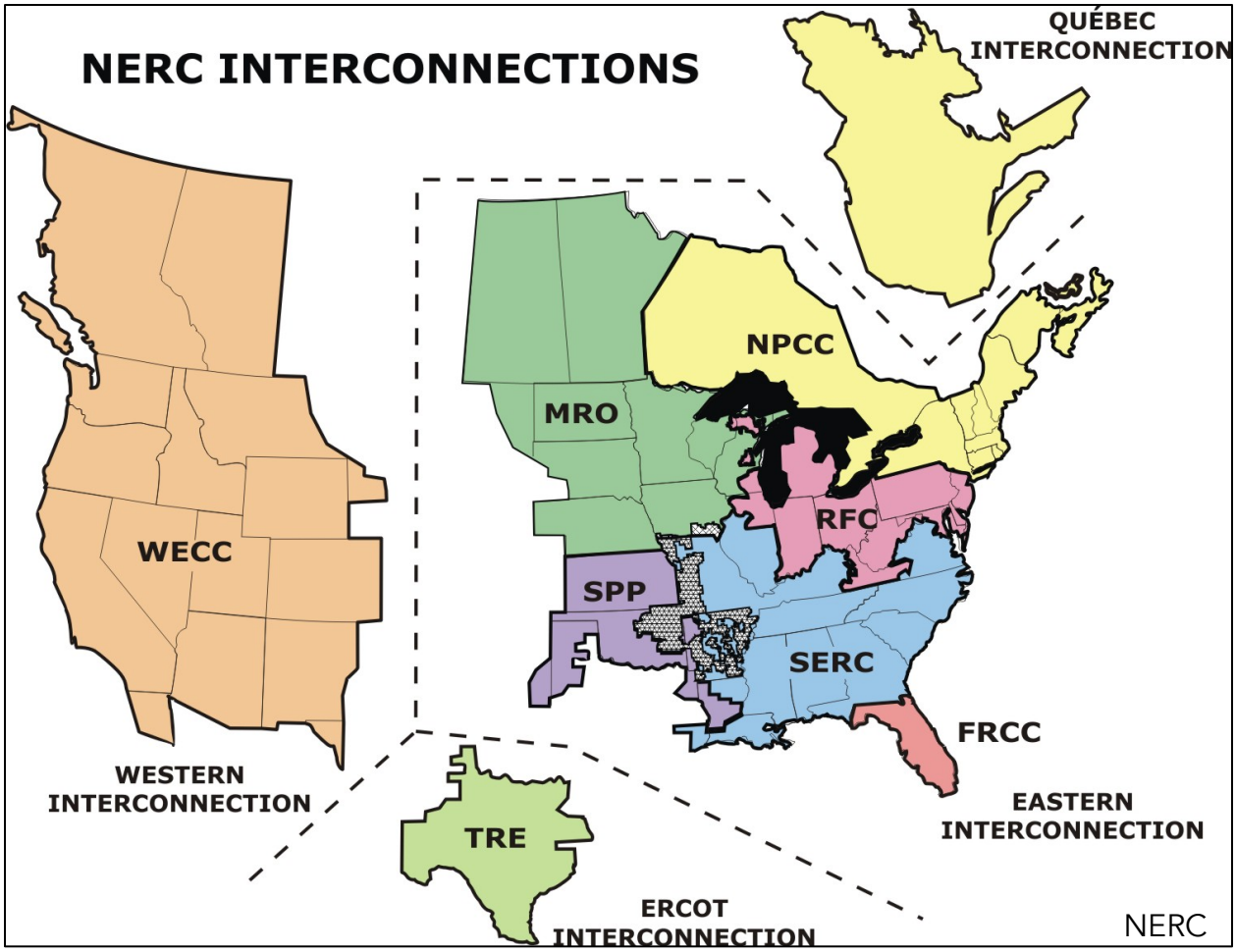
# THE U.S. ELECTRICAL GRID

The U.S. electrical grid, which serves more than 300 million people and is made up of more than 200,000 miles of transmission lines, is one of the most important pieces of infrastructure in the country. Due to the interdependent structure of the components of the grid, a single line outage or system failure, whether due to severe weather, natural or human-made EMP attack, a cyber and/or a physical attack, can cause cascading power outages affecting millions of people and impinging enormous costs on the economy. Despite the number and quality of standards and regulations in the utilities sector, the U.S. electrical grid is a key sector to be examined in terms of not only the various security challenges it faces, but also the legislative and regulatory dynamics that determine communication, information sharing, and cooperation between various levels of government, industry organizations, and utility operators.

## THE BASIC STRUCTURE OF THE U.S. ELECTRICAL GRID

The U.S. electrical grid is composed of 10 power markets that are connected by three systems: the Western Interconnect (from the West Coast to Montana, Wyoming, Colorado, and New Mexico), the Eastern Interconnect (everything east of that line), and the Texas Interconnect (Texas only). While the Western and Texas Interconnects are managed by one reliability council each, the Eastern Interconnect is divided into five different reliability councils. Each power market is composed of various power generation plants, high voltage transmission lines, and large transformers that "step down" the high voltage power into lower voltage power for transmission to the consumer. Within each market, private utilities providers, whose power plants and distribution networks are made up of hardware and software sourced from multiple suppliers, are responsible for the generation, transmission, and distribution of power. These utility operators include investor-owned utilities (IOUs) with multistate operations and significant economies of scale; federally-owned operators like the Tennessee Valley Authority; smaller rural electric cooperatives; or municipal power companies, often referred to as Public Power Districts or Public Utility Districts.

The multitude of actors involved in the generation and delivery of power, combined with the various governmental and industry-based organizations responsible for insuring the reliability and security of the electrical grid, requires careful examination in ensuring that the U.S. grid is protected from a number of man-made and natural threats.




## GRID SECURITY ENTITIES

### FERC & NERC

In the United States, individual utilities are responsible for grid security. Providing oversight and regulation are the Federal Energy Regulatory Commission (FERC) and the North American Energy Reliability Company (NERC). FERC is responsible for regulating the transmission, distribution, and sale of electricity within the 10 power markets of the United States. Through civil penalties and other methods, FERC enforces regulations on the energy industry, though it does not regulate the physical construction of electric plants, or any aspect of nuclear power generation. Within the Energy Policy Act of 2005, mandatory reliability standards had to be established and enforced through cooperation between FERC and the designated Electric Reliability Organization (ERO). NERC has been designated as the ERO, and develops and enforces FERC approved reliability standards to the 10 power markets and 3 interconnects within the US.

NERC is not a federal agency, but rather a private nonprofit with a board of directors which, through its certification as the United States' ERO, has been charged with proposing new reliability standards and developing voluntary "best practices" guidelines for energy companies to follow. NERC acts as an independent, audited, self-regulated electric reliability organization, which uses the subject matter expertise of its members to suggest new policies to FERC, or make unilateral decisions about the voluntary guidelines for electrical providers.

Even with their creation, many of the NERC standards are only being implemented on the mandatory level, which still leaves the grid vulnerable to multiple types of threats, demonstrated by the results presented in the *Electrical Grid Vulnerability* report by Congressmen Markey and Waxman. In addition, that report found that some utilities actually did implement voluntary standards, but this was not a universal practice. As a result, it is almost impossible for NERC to audit companies on an equal level because of the large variation in how these standards are implemented.

NERC also houses the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which is described in further detail below. Separate from its role in ensuring standards compliance, this information sharing capacity complements NERC's role as the designated ERO.

Still, based on the varied legislative proposals there are political questions about the ability of NERC to ensure the needed security standards. During this project's discussions with participants from government and the utility industry, as well as our research, it was found that further regulatory actions resulting from legislative action may be counterproductive, as the increasingly complex threat environment requires rapid information sharing, exchanges of personnel and equipment, and incentives for new technology implementation. Resorting to a regulatory hammer is likely to hamper these efforts and reduce trust between utilities, their regulators, and policymakers.

## DEPARTMENT OF HOMELAND SECURITY & DEPARTMENT OF ENERGY

The Department of Homeland Security (DHS) and the Department of Energy (DOE) play key roles in current efforts to secure the electrical grid, as well as in many of the proposed legislative and regulatory solutions. The Department of Homeland Security coordinates security information and preparedness for the nation's critical infrastructure, while the Department of Energy serves as the sector specific lead agency for grid security.

In cooperation with law enforcement and the intelligence community, these agencies can ensure that all aspects of the grid have access to real-time information and the ability to share that information. With responsibility for critical infrastructure protection, DHS has been involved in a wide range of activities for electrical grid security from physical and cyber threats. In the area of cybersecurity, DHS runs both the United States Computer Emergency Readiness Team (US-CERT) and the National Cybersecurity and Communication Integration Center (NCCIC).

Currently, DHS and DOE are also pursuing programs like TAXII (Trusted Automated eXchange of Indicator Information) and CRISP (Cybersecurity Risk Information Sharing Program) that allow for automated, real-time information about cybersecurity threats. Currently, DOE and the National Laboratories are working on better implementing these tools, alongside the implementation of cybersecurity standards by the National Institute of Standards and Technology (NIST), which is part of the Department of Commerce. Furthermore, with the model of programs like *Kaleidoscope,* used by the U.S. Secret Service during Presidential travel, there are ongoing programs to improve communication and cooperation between the government and private sector to mitigate threats.

In addition to these security roles, the DOE is the lead agency on the "Federal Smart Grid Task Force," which includes DHS, as well as FERC, NIST, the EPA, the Department of Defense, the Department of Agriculture, the FCC, the Department of State, the National Energy Technology Laboratory, and the National Trade Administration. Through this interagency process, the federal government continues to set the standards for the implementation of "Smart Grid" technologies.

## INFORMATION SHARING & ANALYSIS CENTERS (ISACs)

In 1998, under PDD-63 from President Bill Clinton, the Electricity Sector ISAC (ES-ISAC)—along with ISACs for seven other critical infrastructures—was created to provide a clearinghouse for information regarding the security of the electric sector. Operated by NERC, the ES-ISAC provides utilities with information about physical and cyber threats, as well as strategies for addressing vulnerabilities.

Two important roles of the ES-ISAC are its coordination with connected utilities in Mexico and Canada and its coordination with the ISACs of other critical infrastructures upon which the electrical grid relies for its operation. This allows for coordinated action regarding threats that may target water or telecom systems, for example, that would disrupt grid operations.

# ANALYSIS OF INCIDENTS

## CYBER INCIDENTS

### TYPES OF CYBERATTACK

As threat actors are becoming more advanced, the attacks perpetuated against computer systems are increasing in frequency, intensity, and variety. Specific attacks such as data interception, denial of service (DDoS), data alteration, or a cyber "drive by shooting," have been used by groups, individuals, or nation-states depending upon their strategic objective. Additionally, many of the viruses that have caused substantial damage to critical facilitates across the world were specifically designed to compromise Supervisory Control and Data Acquisition (SCADA) systems.

### THE AURORA TEST

As threat actors continue to develop their capabilities, the threat of a joint cyber-physical attack on our electrical grid increases in probability. In 2007, researchers at the Idaho National Lab conducted the Aurora test, in which a virus manipulated the computer network systems that controlled diesel generators. The controlled test involved the opening and closing of circuit breakers, which resulted in an out-of-synchronism condition. Specifically, the out-of-phase synchronism or out-of-phase condition can place stress upon the mechanical components of rotating equipment in generators, causing them to fail.[1]

This test is significant because it not only identified a major vulnerability, but also demonstrated the ability for a computer virus to manipulate grid systems and cause physical damage. While this initial demonstration occurred in a controlled environment, it provided evidence of how future cyberattacks might seek to use vulnerabilities in grid control equipment to cause significant physical damage to grid components.

[1] Marcos Donolo, Armando Guzman, Venkat Mynam, Doug Salmon, & Mark Zeller, " Mitigating the Aurora Vulnerability with Existing Technology," *Schweitzer Engineering Laboratories, Inc.* 2009,

## STUXNET

Starting in 2006, the U.S. government conducted a cyberwarfare initiative, code-named Olympic Games. The Stuxnet virus, which was discovered in June 2010 in Iran and infected over 100,000 computer systems throughout the globe, was developed in a joint-program between the U.S. Intelligence Community and Israel's Unit 8200.[2]

The virus was composed of two separate attacks, which destroyed almost a fifth of Iran's nuclear centrifuges at the Natanz Nuclear Power Plant. The initial attack, referred to as Duqu, "was designed to secretly 'draw the equivalent of an electrical blueprint of the Natanz plant' to understand how the computers control the centrifuges used to enrich uranium."[3] As a result, U.S. officials obtained specific and precise information concerning the physical design of the centrifuges and their interactions with SCADA systems.[4]

The second wave of attack utilized those blueprints by using a specific code uploaded to thumb drives, which was designed to attack the Simens Simatic WinCC SCADA systems by intercepting commands from Human Machine Interface (HMI) software. The Stuxnet virus intercepts commands sent to high-speed frequency-converters, which are devices that control functions, such as motors. Ultimately, the Stuxnet virus revolutionized cyber warfare because it was the first cyber-weapon to target industrial facilities. Additionally, the virus was so destructive due to its ability to physically damage infrastructure by compromising SCADA systems.

## FLAME

After Stuxnet demonstrated its devastating nature, researchers began to develop viruses which would utilize the interconnected nature of SCADA systems to critical physical infrastructure. Another component within Olympic Games was the development of the Flame virus, which was discovered in May of 2012 after infecting computers in Israel, Sudan, Syria, Saudi Arabia, Egypt, Lebanon, and Iran. Researchers concluded that the virus had gone undiscovered for almost five years due to its

---

[2] Michael B. Kelley, "Obama Administration Admits Cyberattacks Against Iran are Part of Joint US-Israeli Offensive," *Business Insider,* June 1, 2012, http://www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2012-6#ixzz1wYnaa3jK

[3] Ibid.

[4] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

complex nature and ability to evade detection by posing as a routine Microsoft software update.[5]

Similar to Stuxnet/Duqu, Flame also compromised Iranian SCADA systems through cyber-sabotage, specifically targeting the Iranian Oil Ministry and Iranian National Oil Company. The malware monitored and mapped out the country's computer networks through the replication of controls and daily tasks associated with HMI functions. Flame has the ability to log keyboard strokes; take screen shots; activate microphones and cameras; obtain geolocation data from images; and receive and send commands and data through Bluetooth wireless technology. Not only is the Flame virus 20 megabytes, but it "contains multiple libraries, SQLite 3 databases, various levels of encryption—some strong, some weak—and 20 plug-ins that can be swapped in and out to provide various functionality for the attackers."[6] Researchers at Kaspersky Lab who discovered Flame stated that this virus has similarities to Stuxnet/Duqu, yet is considerably more complex.

## SHAMOON

In August of 2012, on the Islamic Holy Day of Lailat al Qadr, the computer network of Saudi Aramco was attacked by a self-replicating virus, which compromised approximately 30,000 of its Windows-based machines. The malware, referred to as Shamoon, "erased data on three-quarters of Aramco's corporate PCs—documents, spreadsheets, emails, files—replacing all of it with an image of a burning American flag."[7] Unlike Stuxnet, Shamoon did not result in any physical destruction to infrastructure, yet the virus weakened the business processes of the company by deleting drilling and production data.

According to researchers who studied the virus, Shamoon consisted of three modules: the dropper module or main component, which is the source of the initial infection; the wiper module, which destroyed and eliminated data on the infected computers; and the reporter module, which sent information back to the attacker. Additionally, Shamoon was not able to infiltrate the industrial control system computers involved in

---

[5] Damien McElroy & Christopher Williams, "Flame: World's Most Compex Computer Virus Exposed," *The Telegraph,* May 28, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html

[6] Kim Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers," *Wired,* May 28, 2012, http://www.wired.com/2012/05/flame

[7] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times,* October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=1&

refining or drilling operations and demonstrates the necessity for companies to separate computer systems used for "general business operations and those monitoring and controlling upstream and downstream operations."[8]

An organization called The Cutting Sword of Justice took responsibility for the cyberattack against Saudi Aramco. Although a direct link to the group and Iran was not officially made, many believe that Shamoon was the Iranian response to the sanctions which restrict the export of oil. As a result, Saudi Arabia has the capacity to produce approximately 10 million barrels per day, while much of Iranian oil sits unsold.

## HEARTBLEED

In the spring of 2014, the Heartbleed Bug was found to be a security vulnerability within OpenSSL software, which had infected over 500,000 websites including Yahoo and OKCupid. This flaw let hackers access the memory of data servers, leaving personal data such as passwords, credit card information, and usernames vulnerable. A Secure Sockets Layer, or Transport Security Layer, is the most basic "encryption standard [widely] used by websites that need to transmit the data that users want to keep secure."[9] On occasion, a computer will want to check that there is another computer at the end of its secure connection, and a small package of data—or a "heartbeat"—will be sent out requesting a response. Due to a "programming error in the implementation of OpenSSL, the researchers found that it was possible to send a well-disguised packet of data that looked like one of these heartbeats to trick the computer at the other end into sending data stores in its memory."[10]

A researcher at Google and the security firm Codenomicon discovered the flaw in OpenSSL and confirmed that the bug had been active for at least two years. Due to the highly sophisticated nature of the bug, hackers were able to steal encryption keys used by websites to secure personal information. Additionally, the Heartbleed Bug demonstrated the advanced nature of cyberattacks and how "zero day" exploits, due to poor coding, can go unnoticed for a long period of time.

---

[8] Christopher Bronk & Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival: Global Politics and Strategy* 55 (2013) 81-96

[9] Kyle Russell, "Here's How to Protect Yourself from the Massive Security Flaw That's Taken Over the Internet," *Business Insider,* April 8 2014, http://www.businessinsider.com/heartbleed-bug-explainer-2014-4

[10] Ibid

### ENERGETIC BEAR

Most recently, electrical grid infrastructure within the United States and Europe has come under attack from a group of Russian hackers known as 'Dragonfly'. Since 2011 the group has been conducting various cyberattacks, typically classified as espionage, against European governments, defense contractors, and U.S. health care firms. As of late, Dragonfly has been conducting Stuxnet-type attacks against the industrial control systems found with petroleum pipeline operators, grid operators, electricity generation firms and other critical energy companies.[11]

Dragonfly has developed two Remote Access Trojans (RAT) to install malware on computers, which gives hackers access and control over the infected computer. These attacks, referred to as "Energetic Bear," "are centered on extracting and uploading stolen data, installing further malware onto systems, and running executable files on infected computers…[and] running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloguing documents on infected computers."[12] In addition to the RATs, the group has utilized other attack vectors such as spear phishing/email spam, watering hole attacks/exploit kits, and other trojanized software to destroy the integrity of specific systems. Although the specific motivation for these attacks is unknown, multiple researchers have stated that the RATs utilized by Dragonfly are too advanced and the attacks "bear the hallmarks of a state-sponsored operation."[13]

## PHYSICAL INCIDENTS

### 2003 NORTHEAST BLACKOUT

In August of 2003, a massive blackout shut off the lights to approximately 50 million Americans throughout the Northeast and Midwest. Due to the interconnected nature of the electrical grid, customers in Ontario and Toronto, Canada experienced a blackout. Due to the heat of the high current running through power lines and their proximity to over grown trees, many transmission lines in Northern Ohio experienced overloading. In addition, a software bug at a FirstEnergy facility in Ohio caused the

---

[11] Amy Thomson & Cornelius Rahn, " Russian Hackers Threaten Power Companies, Researchers Say," *Bloomberg,* July 1, 2014, http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms.html

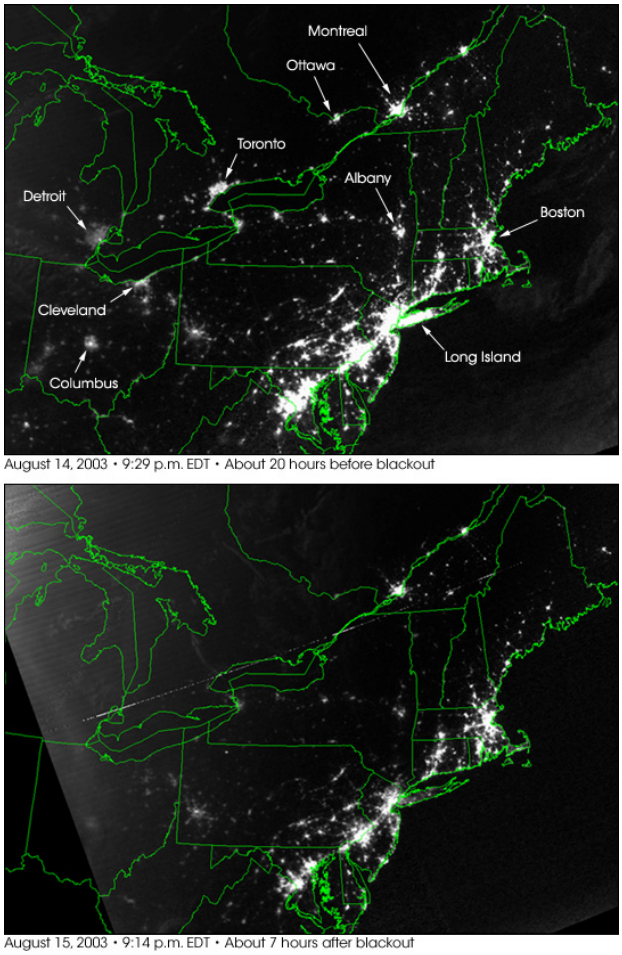
[12] "Emerging Threat: Dragonfly/Energetic Bear – APT Group," *Symantec,* June 30, 2014, http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group

[13] Ibid.

warning alarm system to fail. As operators tried to identify the source of their issues, three other lines shut down, which forced other power lines to carry more power than they could handle. The strained system eventually gave way and resulted in a cascading failure throughout the Northeastern United States and Southeast Canada.[14] All systems were automatically transferred to a backup system, which subsequently failed as well.[15]

One of the first problems occurred to the Stuart-Atlanta 345-kV transmission line, which tripped off-line due to contact with a tree. Energy loads shifted automatically, but this process put other 345-kV lines under stress. As a result, utilities in Ohio began to shift loads from Michigan, but this began to trip other transmission lines throughout the two states. This resulted in multiple power surges to power plants, 345-kV lines, such as the Tidd-Canton Central line and the Hampton-Thetford line, and to major interconnections, including the Star-South Canton and Oneida-Majestic.[16]

The resulting failure throughout the Midwest traveled to the Northeast as sections of the electrical grid experienced surges and overvoltage. Major cities such as Albany, Hartford, New York City, Detroit, and Cleveland all experienced widespread electrical failures to over 256 power plants.[17] Crews were unable to restore power for 4 days in some parts of




*NASA imagery illustrating the areas affected by the 2003 Northeast Blackout.*

[14] JR Minkel, "The 2003 Northeast Blackout – Five Years Later," *Scientific American,* August 13, 2008, http://www.scientificamerican.com/article/2003-blackout-five-years-later/

[15] "Northeast Blackout of 2003," *The Energy Library,* 2009, http://theenergylibrary.com/node/13088

[16] "How and Why the Blackout Began in Ohio," *The National Electric Reliability Corporation,* April 4, 2004, http://www.nerc.com/docs/docs/blackout/ch5.pdf

[17] Jaime Holguin, "Biggest Blackout in U.S. History," *CBS News,* August 15, 2003, http://www.cbsnews.com/news/biggest-blackout-in-us-history/

the United States, and Ontario suffered from rolling blackouts for over a week after the incident.

In response to these events, FERC set new reliability standards to avoid another blackout in the future. FERC turned its attention to three main issues: trees, training, and tools. Personnel working to restore power would have to comply with new training standards, and were equipped with new tools. Additionally, FERC imposed mandatory regulation that trees be kept away from transmission lines.[18]

## METCALF, CALIFORNIA SUBSTATION ATTACK

In April of 2013, multiple individuals conducted a "military style raid" upon the PG&E Metcalf Substation in San Jose, California.[19] Before the attack began, the perpetrators cut fiber-optic phone lines, which not only disrupted service to customers, but made it more difficult for utility personnel to alert emergency services. Cell phones and landlines were also affected in the San Jose area. [20]

*Surveillance footage released by PG&E shows the sparks from bullets hitting the substation equipment.*

The assailants used assault rifles to fire over 100 shots at the banks of transformers from outside the chain-link fence, critically damaging over a dozen. The shots were aimed strategically, as they were not meant to explode the transformers, but rather to severely damage the equipment by slowly draining cooling oil.[21]

PG&E was able to avoid a blackout by transferring loads from power plants in Silicon Valley but customers had to conserve power until workers were able to repair the station and obtain new transformers.[22] It took workers 27 days to return the station to

---

[18] "Northeast Blackout of 2003," *The Energy Library,* 2009, http://theenergylibrary.com/node/13088

[19] Shane Harris, "'Military-Style' Raid on California Power Station Spooks U.S.," *Foreign Policy*, Dec. 28, 2013, http://complex.foreignpolicy.com/posts/2013/12/24/power-station-military-assault

[20] JR Minkel, "The 2003 Northeast Blackout – Five Years Later," *Scientific American,* August 13, 2008, http://www.scientificamerican.com/article/2003-blackout-five-years-later/

[21] Evan Halper & Marc Lifsher, "Attach on Electric Grid Raises Alarm," Los Angeles Times, Feb. 6, 2014, http://www.latimes.com/business/la-fi-grid-terror-20140207,0,5892405.story#axzz2t2mkWwrd

[22] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," Wall Street Journal, Feb. 18, 2014, http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304851104579359141941621778.html

full operation. Even though the substation is located in a remote location, only a chain-link fence and multiple cameras secure the area. As a result, it was easy for individuals to enter the premises and target certain components that are imperative to the grid's functioning. The FBI is still attempting to uncover who is responsible and why this highly coordinated attack occurred. Although the FBI does not suspect terrorism, Jon Wellinghoff, FERC chairman at the time of the attack, disagrees with that assumption. [23]

This attack marks the largest domestic act of potential terrorism on the energy grid. After noticing the vulnerability of the Metcalf Substation, law makers have stated their renewed concern over the vulnerabilities of substations, most of which are easily accessible by those who wish to do it harm. Prior to the Metcalf incident, attacks on utility equipment in the U.S had links to metal thieves, unsatisfied employees, or hunters who occasionally took pot shots at small transformers on utility poles.[24]

## KNIGHTS TEMPLAR DRUG CARTEL ATTACK

In October 2013, members of the Knights Templar drug cartel attacked 18 power stations throughout the Mexican state of Michoacán. [25] In a sophisticated and coordinated attack, members of the cartel used guns and Molotov cocktails to disable electrical substations in 11 cities and towns throughout the state. Officials confirmed that 5 people were killed in the attacks, yet the official cause of death is unknown.[26] Authorities reported that 420,000[27] residents were left without power for 15 hours.[28] The day after the incident 40 percent of the affected areas were still without power.[29] Michoacán is influenced by the drug cartel far more than by laws, as it is one of Mexico's main sources for marijuana, thus sparking the drug trade in the area. The Knights Templar's base is in the capital city of Apatzingán, which was the target of these attacks.[30]

---

[23] "Threat to the grid? Details emerge of sniper attack on power station," *Fox News,* February 6, 2014, http://www.foxnews.com/politics/2014/02/06/2013-sniper-attack-on-power-grid-still-concern-in-washington-and-for-utilities/

[24] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *The Wall Street Journal,* February 5, 2014, http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Tracy Wilkinson, "Attackers in Mexico blow up nine electrical plants," *Los Angeles Times,* October 27, 2013, http://articles.latimes.com/2013/oct/27/world/la-fg-wn-mexico-blow-up-nine-electrical-plants-20131027

[29] "Mexico Drug Cartel Attack Leaves 11 Towns without Electricity, Knights Templar Suspected," *Huffington Post,* October 28, 2013, http://www.huffingtonpost.com/2013/10/28/mexico-drug-cartel-attack-electricity_n_4168761.html

[30] Jose de Cordoba, "Mexican Farmers form Vigilante Forces to Confront Drug Cartels," *The Wall Street Journal,* November 15, 2013, http://online.wsj.com/news/articles/SB10001424052702303559504579198280757965184

In the months leading to the attack, the Knights Templar was under pressure from vigilante groups that had been fighting to regain power from the cartel in the wake of an increased number of kidnappings and murders.[31] As a result, the incident in October was deemed a retaliatory attack to demonstrate the power of the cartel and authorities commented that this was "clearly an act of terrorism."[32] The Knights Templar used the blackouts as a cover, and set fire to four gas stations in the area. The towns that were hit with the blackouts were also towns that were forming self–defense forces against the cartel. These forces marched on the city of Apatzingán claiming they were responding to the calls of their fellow neighbors; during the protest shooting broke out and two people were wounded.[33] The next day the attacks on the power grid took place in retaliation.[34]

Since the attack on the grid, federal authorities dispatched hundreds of police and military troops to reinforce security in the area. However the "organized criminals are winning the battle against federal and state authorities," claimed Miguel Chavez, head of the National Action Party. He went on to conclude that the violence against the power stations was a very clear act of terrorism.

## ATTACKS ON ENTERGY FACILITIES IN ARKANSAS

Months after the attack on the Metcalf substation in California, there were three consecutive attacks on Entergy Arkansas transformers and substations within Lonoke County, Arkansas. On August 21, 2013, a shackle that secured a 500,000-volt electricity line was cut and over 100 bolts of the support tower were removed, leaving only 5 bolts to hold the tower in place.[35] The tower fell onto a neighboring railroad track, leading to a train severing multiple power lines. As a result, the town of Cabot, Arkansas was left without power. The second in the series of attacks came on September 29, when a fire was intentionally set at the Entergy electricity station in Scott, Arkansas causing around $2 million in damages to the station.[36] The final attack

---

[31] "Mexico Drug Cartel Attack Leaves 11 Towns without Electricity, Knights Templar Suspected," *Huffington Post,* October 28, 2013, http://www.huffingtonpost.com/2013/10/28/mexico-drug-cartel-attack-electricity_n_4168761.html

[32] Nicholas Casey, "Mexican Cartel Retaliates Against Civilians," *The Wall Street Journal,* October 28, 2013, http://online.wsj.com/news/articles/SB10001424052702304200804579163840007600858

[33] Jose de Cordoba, "Mexican Farmers form Vigilante Forces to Confront Drug Cartels," *The Wall Street Journal,* November 15, 2013, http://online.wsj.com/news/articles/SB10001424052702303559504579198280757965184

[34] Jo Tuckman, "Mexican Vigilantes take on Drug Cartels – and worry authorities," *The Guardian,* October 28, 2013, http://www.theguardian.com/world/2013/oct/28/mexican-militias-vigilantes-drug-cartels

[35] "Arrest made over Arkansas Power Grid Attacks," *CBS News,* October 14, 2013, http://www.cbsnews.com/news/arrest-made-over-arkansas-power-grid-attacks/

[36] Ibid.

occurred in October, in Jacksonville, Arkansas, where a First Electric Cooperative power pole was damaged and then pulled down by a tractor. This incident resulted in the downing of a 115,000-volt transmission line, causing power outages for over 9,000 customers.[37] The power lines targeted all link a high-voltage transmission line with either a switching station or substation. Not only are these lines extremely vulnerable, but could easily be found on Google Maps.[38]

The FBI, who had been investigating these attacks since August, eventually arrested a man from Arkansas, Jason Woodring, and charged him with the destruction of an energy facility.[39] Police arrested Mr. Woodring after responding to an explosion under power lines near his home. He was convicted of 8 counts related to his attacks on the power grids and faces the potential of life in prison and five years of supervised release following any lesser prison stay, as well as a $250,000 fine.[40] Authorities have concluded that Mr. Woodring seemed to be acting alone, and did not have connections to a larger terrorist organization.

## NOGALES, ARIZONA SUBSTATION ATTACK

In June of 2014, a makeshift bomb was placed next to a 50,000 gallon diesel tank at a power station in Nogales, Arizona. The bomb, described as a "crude incendiary device," was placed under the valve of the diesel tank and ignited. Police believe the attackers entered the substation just before maintenance workers locked up the station, and they left when the workers returned to the station the next day. The Valencia Generating Station, the target of the attack, is a small peaking facility that is only used during extreme temperatures in summer and winter.[41] The Valencia plant serves about 30,000 people and is adjacent to a substation, which is important for balancing the regional power supply.

The four turbines at the plant were not running at the time of the incident, and electricity supplies were not affected. The turbines are primarily fueled by natural gas

---

[37] Ibid.
[38] William Pentland, "Weekend Attacks on Arkansas' Electric Grid leave 10,000 without Power; 'You Should Have Expected U.S.'" *Forbes,* October 7, 2013, http://www.forbes.com/sites/williampentland/2013/10/07/weekend-attacks-on-arkansas-electric-grid-leave-10000-without-power-you-should-have-expected-u-s/
[39] Chelsea J. Carter, "Arkansas man charged in connection with power grid sabotage," CNN, Oct. 12, 2013, http://www.cnn.com/2013/10/08/us/arkansas-grid-attacks/
[40] "Federal Grand Jury Returns Eight-Count Indictment Against Jason Woodring," *Federal Bureau of Investigation,* November 6, 2013, http://www.fbi.gov/littlerock/press-releases/2013/federal-grand-jury-returns-eight-count-indictment-against-jason-woodring
[41] "Sabotage at Nogales station puts focus on threats to grid," *AZ Central,* June 13,2014, http://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/

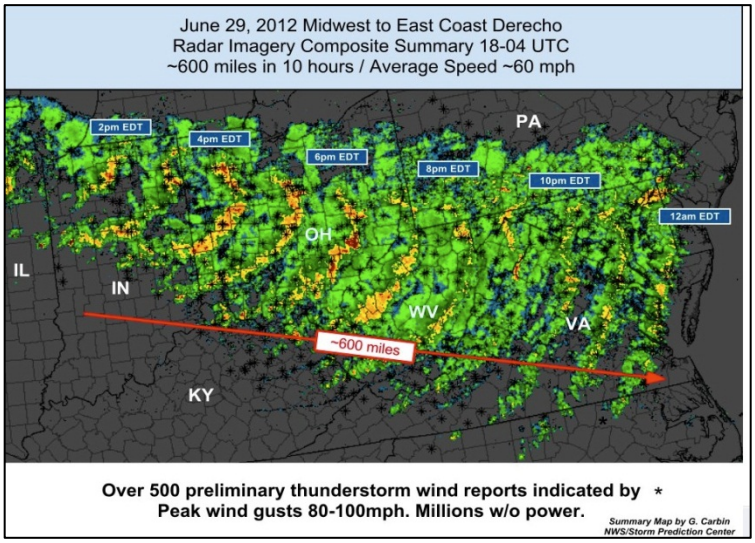
and the diesel fuel that was targeted serves as an emergency source for the turbines. The FBI is currently investigating this incident in conjunction with two other incidents in Sahuarita, located North of Nogales: the first involved individuals attempting to cut power lines and the second incident involved target shooters who were seen on security cameras near a substation. [42] All the stations targeted by these events were owned by the UniSource Energy Services, which is a subsidiary of UNS Energy, based in Tucson, Arizona.

Law enforcement and UniSource Energy Services do not believe there was a specific target, but rather the saboteurs wanted to carry out an attack on the plant.[43] It is also believed that they had some knowledge of the inner workings of the plant. Authorities have not arrested any individuals connected to the attack.

## SEVERE WEATHER

### 2012 MID-ATLANTIC DERECHO

During the summer of 2012, a storm system referred to as a derecho brought a series of thunderstorms, hurricane force winds, and a heat wave to the Ohio Valley and Mid-Atlantic states. The storm traveled 600 miles in only 10 hours, which left approximately 4.2 million customers without power throughout 12 states, with West Virginia being hit the hardest. In many cases power was not restored for over a week following the storm. Overall, the multi-day derecho resulted in $2.9 billion dollars-worth of damages and 28 deaths.[44]




*National Weather Service composite radar imagery illustrates the scope and speed of the 2012 Derecho.*

[42] Ibid.
[43] Ibid.
[44] "A Review of Power Outages and Restoration Following the June 2012 Derecho," U.S. Department of Energy, August, 2012, http://energy.gov/sites/prod/files/Derecho%202012_%20Review_0.pdfithi

Due to variances in the path and intensity of the storm, the highest reported electrical outages varied by state. "For example, West Virginia had 63 percent of electric utility customers without power after the storm, followed by Maryland with 33 percent, Virginia with 32 percent, and the District of Columbia with 25 percent."[45]

Returning power to different states also varied immensely. After one day only 6 percent of Washington, D.C customers had their power restored, whereas over 90 percent of customers in Illinois received power after a single day. These variances were dependent upon a number of factors including the recovery capabilities of utilities, additional storms resulting in a heat wave and/or fallen trees, and the intensity and range of damage to the components of the electrical grid in each state. Although the initial recovery process was at a similar pace compared to other storms, the process slowed after the first day and total restoration took longer than storms that affected similarly sized areas—such as Hurricanes Irene and Ike. The stagnant pace was due to the lack of advance warning given to utilities and state governments, as the storm developed over 18 hours from thunderstorm cells near the Chicago area into a wave of severe storms stretching from southern New Jersey to North Carolina.

Unlike Hurricanes Ike and Irene, NOAA estimated low to moderate winds across Illinois, Indiana, Southern Michigan, Western New York, and Pennsylvania. Realizing faults in initial estimates, NOAA updated the report only three hours before the storm hit, calling for significantly stronger winds, an increased area to be affected, and thunderstorms.[46]

## SUPERSTORM SANDY

Also occurring in 2012, Superstorm Sandy was a category 3 hurricane that caused extensive damage to the Eastern seaboard, specifically to New York and New Jersey, resulting in 159 deaths. When the storm first hit, 8.5 million customers were without power and a week after the storm initially hit, there were still 1.3 million without power.

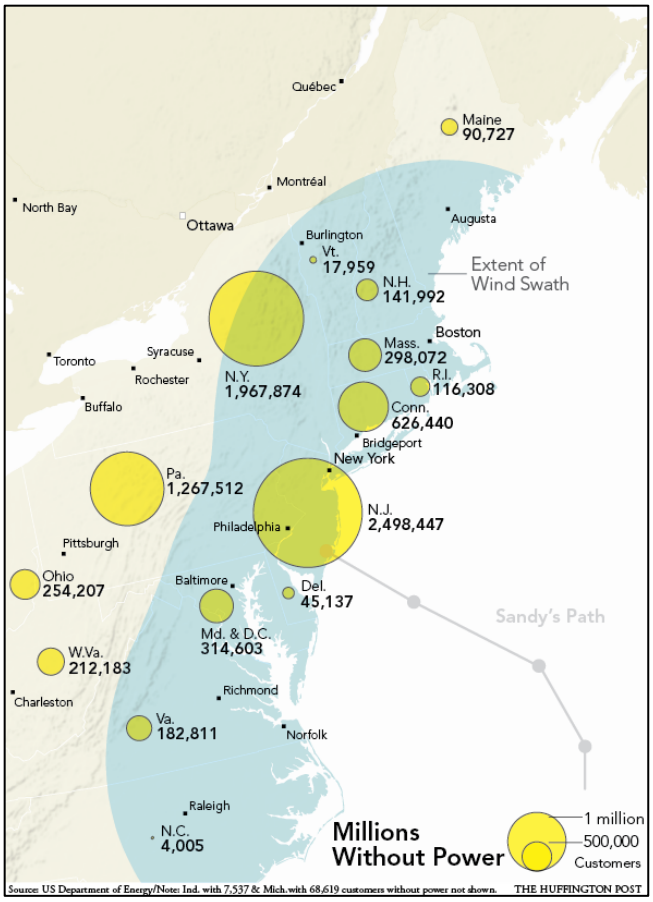
Superstorm Sandy resulted in $65 billion in overall damages, $14-26 billion in electrical outage costs, and approximately $8.3 billion in business losses in New Jersey, making it the second most expensive storm in U.S. history, behind Katrina.

[45] Ibid.
[46] Ibid.

The majority of the damage that occurred to electrical utility infrastructure was caused during the storm surge. Damage from floodwater can rust metals, destroy insulation, damage interruption capabilities, and trip units in molded-case circuit breakers can be impaired.

Systems in an urban area where many vital grid components are placed underground—alongside many other utilities' infrastructure—are especially vulnerable to flooding or sea level change caused by storm surge and other phenomenon.

Additionally, components such as wire, cable, ground-fault circuit interrupters, lighting fixtures, surge protectors, motors, transformers, and other equipment must be replaced.[47] For example, the ConEd substation in New York City on the East River on 14th Street exploded due to flooding.




*This image, from the Huffington Post, illustrates the wind field from Superstorm Sandy and the numbers without power.*

The damage to the substation caused 250,000 customers to lose power.[48] In an attempt to protect electrical equipment, PSE&G prematurely cut off service to approximately 500,000 customers due to flooding at multiple substations.[49]

Even two weeks after the storm approximately 120,000 customers in New York and New Jersey were without power.[50] Even if power was running through certain neighborhoods, some businesses and homes were too damaged to connect to the power source. After Sandy hit the East Coast, the Long Island Power Authority (LIPA)

[47] Jeff Griffin, "Disaster After Disaster?" *Electrical Contractor*, May 2006, http://www.ecmag.com/section/safety/disaster-after-disaster

[48] Matt Sledge, Joy Resmovits, & Joe Van Brussel, "Hurricane Sandy Utility Outages May be Worsened by Underinvestment, Lack of Planning," *Huffington Post*, November 2, 2012, http://www.huffingtonpost.com/2012/11/01/hurricane-sandy-utility-outages_n_2053120.html

[49] Ibid.

[50] Ibid.

was heavily criticized for a lack of adequate response, as over 55,000 customers either did not have power or could not safely connect because local grids were still flooded.[51] A large obstacle for the LIPA was a lack of communication between the company and customers regarding the estimated dates that power was to be restored.

As returning power to those customers affected by Superstorm Sandy was a tiresome and difficult process, electrical utilities have begun to reevaluate their weather response plans and invest in new technology to harden the grid and increase reliability.

*This aerial photograph illustrates the blackout following Hurricane Sandy that affected Lower Manhattan and parts of Midtown.*
*Photo Credit: Iwan Baan for New York Magazine*

[51] Ibid.

## FUKUSHIMA

On March 11, 2011, the Fukushima I Nuclear Power Plant in Fukushima, Japan experienced a catastrophic failure, which triggered the subsequent shutdown of three of its six nuclear reactors and the leakage of appreciable amounts of radioactive matter. A major earthquake, which in turn led to a tsunami, was the cause of what would become the biggest nuclear meltdown since the Chernobyl disaster in the Ukraine in 1986. One of the twenty-five most powerful plants in the world, Fukushima Daiichi has a total of three reactors with a combined power of 47 gigawatts. The tsunami caused the reactors to instantly lose their power supply and cooling mechanisms, leading to cascading shutdowns. According to the World Nuclear Organization, "eleven reactors at four nuclear power plants in the region were operating at the time and all shut down automatically when the quake hit."[52]

The incident was so devastating largely due to the lack of oversight by the Tokyo Electric Power Company (TEPCO) officials who ran it. They ignored the International Atomic Energy Agency (IAEA), who had warned in 2008 that their safety guidelines were outdated and that the Japanese reactors were only designed to withstand magnitude 7.0 tremors—not a 9.0 like the Tōhoku earthquake.[53]

There is ongoing debate about whether the risk of radiation poisoning could possibly have outpaced over 1,000 deaths that occurred during the post-incident evacuation of around 160,000 people. According to the World Nuclear Organization, "the high rate of these deaths continues three years later as the evacuation is maintained for about 135,000 people—apparently some 75,000 from the nuclear accident and 60,000 from the natural disaster itself."[54] France's Institute for Radiological Protection & Nuclear Safety (IRSN) estimated that, based on airborne measurements, the radiation would not exceed natural background levels. However, there is disagreement about what constitutes a low-enough level for evacuees to return, and continuing effects remain an unknown quantity. Three years after the incident, the area closest to the plant remains a "red zone."

Massive radiation leakage into the water remains the most pressing issue for the cleanup process, which is expected to span decades. On July 9, 2013, TEPCO officials

---

[52] "Fukushima Accident," *World Nuclear Organization,* June 2014, http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/fukushima-accident/

[53] Christopher Hope & Steven Swinford, "Japan Earthquake: Japan Warned over Nuclear Plants, Wikileaks Cables Show," *The Telegraph,* March 15, 2011, http://www.telegraph.co.uk/news/worldnews/wikileaks/8384059/Japan-earthquake-Japan-warned-over-nuclear-plants-WikiLeaks-cables-show.html

[54] "Fukushima Accident," *World Nuclear Organization,* June 2014, http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/fukushima-accident/

investigated an abrupt spike in cesium 134 and 137 levels in the Pacific Ocean; they suspect contaminated water leakage is responsible for these chemicals reaching 150 and 200 times their legal levels.

This disaster immediately cast a shroud over what many had considered a renaissance in nuclear power. Japan immediately shuttered its nuclear power plants, though as part of Prime Minister Abe's plans for economic growth, many are being restarted. In Germany, Fukushima reignited political opposition to nuclear power, resulting in a U-turn by the government of Chancellor Angela Merkel when a phased shutdown of German nuclear power was announced.

As the cleanup at Fukushima continues, the lessons learned from this disaster—as well as the political ramifications—will continue to color the debate about nuclear power's role in the future electricity generation portfolio.

## ELECTROMAGNETIC EVENTS

### CARRINGTON EVENT

In September of 1859, Astronomer Richard Carrington observed an enormous group of sunspots in space, which lasted for nearly five minutes. The sunspots Carrington observed were white–light solar flares, essentially a magnetic explosion on the sun. The solar flare produced a global aurora, in which skies across the world were filled with red, green, and purple auroras. Additionally, the flare produced a large cloud of charged particles and detached magnetic loops, referred to as Coronal Mass Ejection (CME), which were sent towards Earth. Due to the intense nature and magnitude of the solar flares, a geomagnetic storm occurred above earth.[55]

When the CME collided with Earth's magnetic field it caused the global bubble of magnetism that surrounds earth to shake. The rapid movement of the fields induced electric currents that surged through telegraph lines, disrupted communications, and discharged sparks which set fire to telegraph papers.[56]

As our society continues to rely upon electronics, the impact of a Carrington Event or major geomagnetic storm could have dire consequences, as demonstrated by the 1989 Hydro Québec storm. During this event multiple transmission lines failed after a

[55] "A Super Solar Flare," *NASA*, May 6 2008, http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/
[56] Ibid.

geomagnetic storm occurred, which caused an extensive power outage to 6 million customers throughout Québec province. Additionally, solar storms have the ability to disrupt GPS navigation, cell phone communication, and radar, which are essential components to the daily functioning of both civilian and military society.

## "STARFISH PRIME" NUCLEAR TEST

*This U.S. Air Force image is of the blast cloud in the upper atmosphere following the Starfish Prime detonation.*

In 1962, the United States conducted the *Starfish Prime* 1.4-megaton nuclear test approximately 20 miles from Johnston Atoll in the Pacific Ocean. The explosion, which occurred at an altitude of 250 miles, affected electronic equipment almost 800 miles away in Hawaii. This nuclear weapons test resulted in a temporary alteration of the intensity and shape of the Van Allen belts, which are energetic particles or radiation belts in the Earth's magnetosphere.[57]

The alteration in the magnetosphere produced an EMP, which disrupted electronic infrastructure essential to the daily functioning of military and civilian personnel. Additionally, the radiation from this test and other high altitude nuclear tests created an artificial radiation belt in the atmosphere that worked in conjunction with the EMPs to damage satellites in lower earth orbit. [58] Long-range radio communication was disrupted for several hours at some frequencies and radio pathways.[59]

As much of our nation's critical infrastructure relies upon electronic devices and microelectronics, a nuclear weapon similar to the magnitude of *Starfish Prime* would have a devastating effect on the security and stability of the United States.

---

[57] "'Starfish Prime', Outer Space," *Comprehensive Test Ban Treaty Organization,* 2014, http://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space/

[58] Ibid.

[59] Jerry Emanuelson, B.S. E.E., "An Introduction to Nuclear Electromagnetic Pulse," *Fururescience, LLC,* http://www.futurescience.com/emp.html

A High-Altitude Electromagnetic Pulse (HEMP) is comprised of three components: the E1 pulse is a fast pulse of intense static electricity that induces high voltages in equipment, along electrical wiring and cables, and can destroy computer and communication equipment; the E2 component has characteristics similar to that of a lightning strike; and the E3 pulse is a long-lasting magnetic signal.

## 1983 QUÉBEC BLACKOUT

One of the largest geomagnetic storms occurred in March of 1989 and led to the collapse of the Hydro-Québec system and the Québec interconnection. Geomagnetic storms are bursts of energy produced by the sun during a CME, which is an occurrence related to a solar flare. The wind plasma that is released during a CME connects with the Earth's magnetosphere causing various changes in the configuration of the planet's magnetic field. This produces geomagnetic-induced currents (GIC), which have the ability to overload electric transformers and power stations.[60]

A massive blackout occurred in a matter of minutes, which resulted in a loss of power to over six million customers. Geomagnetic-induced currents affected protective systems on volt-ampere reactive (VAR) compensators and generator step-up transformers, and permanent damage occurred to a generator step-up transformer at a nuclear station in New Jersey.[61] Additionally, the orbit of satellites was disrupted and high-energy particles invaded some satellites' sensitive electronics, causing 250 recorded anomalies.[62]

Since the blackout, utilities have begun to implement new technology and integrate new methodologies in an attempt to mitigate the effects of future geomagnetic storms. Utilities have recalibrated protection systems, raised the trip level, modified the power system operating procedure, and installed series compensation on power lines to enhance grid stability.[63]

---

[60] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," *NERC*, June 2010, http://www.nerc.com/pa/CI/Resources/Documents/HILF_Report.pdf

[61] "Solar Storm Risk to the North American Electric Grid," *Lloyd's and the Atmospheric & Environmental Research, Inc*, 2013, www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/solar%20storm%20risk%20to%20the%20north%20american%20electric%20grid.pdf

[62] "The Day the Sun Brought Darkness," *NASA*, March 13, 2009, http://www.nasa.gov/topics/earth/features/sun_darkness.html

[63] http://www.hydroquebec.com/learning/notions-de-base/tempete-mars-1989.html

# THREAT ACTORS

On one end of the threat spectrum are state actors. Countries like Russia and China seek to exploit grid vulnerabilities to serve strategic objectives in wartime—notably striking at the U.S. homeland and critical military facilities and systems. For countries like Iran and North Korea, grid vulnerabilities serve as targets for attacks aimed at disruption or asymmetric effects in terms of national, economic, and civil security. Non-state actors target grid facilities for not only the asymmetric efforts, but also to make political statements and challenge perceptions of governance and stability. Finally domestic actors may seek to act in terms of ecological, anarchical, or anti-capitalist motives, while companies must also be aware of the insider threat of disgruntled or otherwise disaffected personnel.

## STATE ACTORS

### RUSSIA

In addition to the United States, Russia is considered to be one of the most capable states at conducting and responding to cyber warfare.[64] While the United States ranks highly on offensive cyber warfare capabilities, experts warn that they are not adequately prepared to defend against a potential cyberattack from a state that possesses advanced capabilities for a cyberattack, such as China, Russia, and even North Korea. As of now, there are no direct, confirmed links between the Russian government and specific attacks. However, as with most government-sponsored cyberattacks, most come from non-state actors, yet enjoy state direction, affiliation, or toleration. Russia has allegedly used its military, secret service, and privately contracted agencies to carry out cyber breaches on other businesses and nations. Based on Russia's known abilities to produce some of the world's best computer hackers, it is safe to assume that Russia's Federal Security Service (FSB) has had teams monitoring organizations and nations.[65]

This was made apparent in the 2007 cyberattacks on Estonia's critical technology infrastructure. The three-week wave of massive cyberattacks was catalyzed by the Estonian government's removal of the Bronze Soldier Soviet war memorial. There were many protests by the Russian population in Estonia, and weeks later, major Estonian

---

[64] Raoul Chiesa, "Hackito Ergo Sum Conference," *Security Brokers and United Nations Interregional Crime and justice Research Institute,* 2013, http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities

[65] "Threats on the Horizon: The Rise of the Advanced Persistent Threat," *Fortinet,* 2013, http://www.fortinet.com/sites/default/files/solutionbrief/threats-on-the-horizon-rise-of-advanced-persistent-threats.pdf

government and business websites began to malfunction. Websites for the Estonian presidency and its parliament were disabled, as well as the government ministry, political parties, newspapers, banks, and other companies. These attacks are referred to as "Distributed Denial of Service" (DDoS) attacks. During a DDoS attack, websites are hit with tens of thousands of visits, which overcrowds the bandwidths for servers running the sites. In the case of Estonia, the DDoS attacks were traced to sources with Russian origins. To date, questions remain as to how much of an enabling role the Russian government played in the attacks.[66] In 2009, the *Wall Street Journal* reported that cyber-spies had penetrated the U.S. electrical grid and had "left behind software programs that could be used to disrupt the system."[67] The spies allegedly came from China and Russia, and while they did not manage to damage the power grid or other infrastructure, officials warned that Russia has attempted to map U.S. infrastructure and could potentially damage the power grid during a crisis or war.[68]

### *Russian Use of Criminal Groups as Proxies*

As organized crime syndicates and cyber-based hackers continue to develop their capabilities, many believe that the Russian government employs these groups as proxies to wage cyberattacks against international targets. In March 2014, Russian forces allegedly used hacking techniques to intercept a U.S. surveillance drone flying over the Crimea region of Ukraine. Hackers were able to disable the connection between the drone and its operator.[69] Since the 2014 Ukraine crisis, American intelligence agencies have been on high alert for cyberattacks aimed at Ukraine. A British-based defense and security company, BAE Systems, reported that dozens of computer networks in Ukraine have been infected for years by a cyber espionage "tool kit" called Snake.[70] While nothing is confirmed, BAE cited circumstantial evidence that the attacks originated in Russia due to Moscow time zone operations and Russian language in some of the code.[71]

---

[66] "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review,* The Elliott School of International Affairs at George Washington University, http://www.iar-gwu.org/node/65

[67] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies, *Wall Street Journal,* April 8, 2009, http://online.wsj.com/news/articles/SB123914805204099085

[68] Ibid.

[69] "Hacked U.S. surveillance drone over Crimea shows new face of warfare," *Homeland Security News Wire,* April 11, 2014, http://www.homelandsecuritynewswire.com/dr20140411-hacked-u-s-surveillance-drone-over-crimea-shows-new-face-of-warfare

[70] David Sanger and Steven Erlanger, "Suspician Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," *New York Times,* March 8, 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=0

[71] "Snake Campaign and Cyber Espionage Tool Kit," Report, *BAE Systems,* 2014, http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

## CHINA

China, along with Russia, is another state known for its alleged hacking of U.S. government systems and corporations. A recent National Intelligence Estimate on economic cyber espionage stated that China was the "most active country in stealing intellectual property from U.S. companies,"[72] and alleged state-sponsored hackers have been accused of infiltrating *Bloomberg, Wall Street Journal, Washington Post*, and other major U.S. news outlets. China is currently pursuing efforts to modernize and improve its military, and is reportedly investing in ways to balance against U.S. military capabilities. According to a 2013 Pentagon report to Congress on China, the country has engaged in cyber espionage as a way to reinforce military strength.[73] Chinese hackers were recently accused in May 2013 of stealing designs for over two-dozen major U.S. weapons systems, including anti-missile and ballistic missile defense systems as well as aircraft and ship designs.[74]

China is alleged to have its own cyber army unit, called "P.L.A. Unit 61398," that has been known to hack into U.S. systems.[75] A study conducted by Mandiant, an American computer security firm, released information attributing members of well-known Chinese hacking groups to the location of the Unit 61398 building area. This has led U.S. agents to believe that the Chinese hacking groups are either part of the Chinese government or they are state-sponsored groups.[76] P.L.A. Unit 61398 has reportedly stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.[77] In addition to targeting U.S. systems, the government of Canada has also been the victim of Chinese-based cyberattacks. In January 2011, multiple Canadian governmental agencies were hit with cyberattacks consisting of phishing emails, which appeared to come from other government employees. In turn, the emails

---

[72] Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign," *Washington Post,* February 10, 2013, http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html

[73] Gopal Ratnam, "Pentagon Accuses China of Cyberspying on U.S. Government," *Bloomberg,* May 7, 2013, http://www.bloomberg.com/news/2013-05-06/china-s-military-ambitions-growing-pentagon-report-finds.html

[74] Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *Washington Post,* May 27, 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

[75] David Sanger, David Barboza, Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times,* Febrary 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all

[76] "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant Intelligence Center Report,* 2013, *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf*

[77] Ibid.

led to hacking of the Treasury Board, Department of National Defense, and the Department of Finance.[78]

Chinese military doctrine has increasingly focused on the concept of what is translated into English as "Informationalized Warfare," which uses cyber, electronic, and other forms of standoff weaponry to interfere with critical infrastructure, communications, and other command and control systems during warfare. Additionally, as encompassed by the use of the term, *shashoujian*, or "Assassin's Mace," Chinese military planners are looking for asymmetric avenues that can quickly disrupt, delay, or paralyze U.S. and allied assets. In terms of grid security, it is worth analyzing whether intrusions into U.S. electrical grid networks originating in China are for the purposes of intellectual property theft or intelligence preparation of the battlefield for a future cyber conflict. It is likely that intrusions targeting generation and SCADA control systems are aimed at gathering intelligence about potential targets, while intrusions that test or analyze more innovative Smart Grid tools are dual purpose activities designed to gain both military intelligence and trade secrets.

Even though China has demonstrated its ability to hack into various government agencies and corporations, the economic partnership may deter both the United States and China from perpetrating a major cyberattack against the other. As China is one of the top U.S. intellectual property thieves and has a military branch dedicated to cyber espionage, it is necessary for the U.S. military to reinforce our cyber defense against Chinese attacks.

## IRAN

Iran provides a serious threat to the country's overall national security, with specific attention to the 16 sectors of critical infrastructure. Although Iran does lack technological sophistication when compared to other threat actors, such as China or Russia, Iran's diligence and tenacity make it just as formidable an opponent. Iran has demonstrated its ability to conduct multiple types of cyberattacks including Computer Network Exploitation, in which sensitive data and information is taken, and Computer Network Attack, in which computer systems and networks are destroyed.

Hezbollah, an Iranian-backed terrorist group, has been known to develop the capacity to conduct a cyberattack and has formed a smaller Cyber Hezbollah sector. Hezbollah

[78] Greg Weston, "Foreign hackers attack Canadian government," *CBC News*, Feb. 17, 2011, http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618

first displayed evolving cyber skills during its 2006 war with Israel and U.S. officials suspect the group's technological abilities have evolved greatly since then.[79] U.S. officials have also received several reports that claim Iranian and Venezuelan leaders were working together to target computer systems at nuclear power plants.[80]

Over a few weeks in late 2012 and early 2013, several American online banking sites were hit by DDoS attacks. The cyberattacks caused the sites to slow or stop functioning, yet returned to operation minutes later. The capabilities required to perpetrate these attacks led U.S. officials to believe Iran was behind the assault. Additionally, the Izz ad-Din al-Qassam hackivist group, an Iranian-affiliated cyber terrorism group, has also been known to cause disruptions in online banking. Overall, Iran and government-sponsored organizations throughout the country are continuing to expand their ability to conduct a major cyberattack.

## NORTH KOREA

The Democratic People's Republic of Korea poses an unpredictable cybersecurity threat to the United States, especially to the critical infrastructure sectors. Even though North Korea has a limited capacity to conduct cyberattacks, the country has stated its intent to conduct Computer Network Attacks.

There have been reports that suggest North Korea has sent top computer science students abroad to develop their skills.[81] Additionally, China has provided much needed technological assistance to North Korea, including regular upgrades to the high–speed Internet lines, and has supplied P'yongyang with advanced computer hardware.[82]

Some of the most destructive cyberattacks and espionage campaigns against South Korea and the United States were conducted by the DarkSeoul gang over a four-year period. The gang, with the support of the North Korean government, targeted banks, news, media, telecoms, and military think tanks. This campaign began with a DDoS

---

[79] Ward Carroll, "Hezbollah's Cyber Warfare Program," *Defense Tech,* June 2, 2008, http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/

[80] Shaun Waterman, "U.S. Authorities Probing alleged Cyberattack Plot by Venezuela, Iran," *The Washington Times,* December 13, 2011, http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all

[81] "North Korea hacker threat grows as cyber unit grows: defector," *Reuters,* June 1, 2011, http://www.reuters.com/article/2011/06/01/us-korea-north-hackers-idUSTRE7501U420110601

[82] Mark Clayton, "In cyberarms race, North Korea emerging as a power, not a pushover," *The Christian Science Monitor,* October 19, 2013, http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover

attack in July 2009 against South Korean and U.S. government and financial websites. "The attacks appeared to emanate from 435 different servers in 61 countries around the world—including South Korea itself."[83] The second wave of attacks included the launch of malicious software that wiped hard drives on systems at one of the largest South Korean banks. Overall, the attacks cost South Korea approximately $750 million in damages.

Some of the trademarks of the DarkSeoul gang's attacks included: "multi-states, coordinated attacks against high-profile targets in South Korea; destructive payloads, such as hard disk wiping and DDoS attacks configured to trigger on historically significant dates; use of legitimate third-party patching mechanisms in order to spread across corporate networks; specific encryption and obfuscation methods; and use of similar command-and-control structures."[84] Additionally, between 2010 and 2011, North Korea increased the size of its cyber warfare unit, going from 500 people to nearly 3,000 people, demonstrating the country's increased interest in cyber warfare.[85]

The attacks that North Korea has conducted demonstrate that the "Hermit Kingdom" has been developing its cyber warfare capacity as a way to asymmetrically confront South Korean and U.S. capabilities.

## NON-STATE ACTORS

### AL-QAEDA

Among terrorist groups, al-Qaeda has been one of the most pervasive in exploiting U.S. resources and infrastructure. The anti-American operational plans of al-Qaeda have started to go beyond 'conventional' physical attacks, as U.S. forces found reason to believe that the terrorist group has been pursuing its cyber warfare capabilities. Computers and manuals full of SCADA system information were discovered at al-Qaeda training camps in 2002. Based on evidence gathered at the camps, al-Qaeda had a "high level of interest" in SCADA devices, and the FBI feared the terrorist group may attempt to target the water supply, wastewater management, and other power

[83] Ibid.
[84] "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," *Symantec*, January 23, 2014, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
[85] "North Korea hacker threat grows as cyber unit grows: defector," *Reuters*, June 1, 2011, http://www.reuters.com/article/2011/06/01/us-korea-north-hackers-idUSTRE7501U420110601

system and industrial operations.[86] Since then, the group has continued to demonstrate its interest in developing cyber warfare capabilities and in a recently released video, an al-Qaeda operative called for an "electronic jihad" against the United States, and compared vulnerabilities in American computer systems to flaws in aviation security preceding the September 11 attacks.[87]

Al-Qaeda has also focused on recruiting skilled members who would be capable of cyberattacks. It was reported that Khalid Sheikh Mohammed, al-Qaeda's arrested operations chief, was an engineering student in North Carolina who later radicalized and moved to the Middle East working for al-Qaeda.[88] Osama bin Laden, the man who masterminded the deadly 9/11 attacks, also carried an engineering degree.[89] An Oxford University study found that graduates from subjects such as science, engineering, and medicine are strongly overrepresented among Islamist movements in the Muslim world.[90] The study also found that among violent Islamist groups, individuals with an engineering education are four times more frequent than we would expect given the share of engineers among university students in Islamic countries.[91] The increased exploitation capability due to the high number of engineers in organizations such as al-Qaeda is one reason among many why cybersecurity in the electrical grid is so important.

## DRUG CARTELS

Drug cartels pose a fairly new and emerging threat to the electrical grid. In the past, drug cartels have been known to attack the infrastructure of multinational companies. "Caballeros Templarios," also known as "Knights Templar," is perhaps one of the more pervasive cartels to attack infrastructure. In 2012, the group admitted responsibility for arson attacks on a Mexico-based subsidiary of PepsiCo, claiming that it was punishment for the company providing cover for government agents.[92] A separate

---

[86] Kevin Anderson, "US 'fears al-Qaeda hack attack,'" *BBC News,* June 27, 2002, http://news.bbc.co.uk/2/hi/science/nature/2070706.stm

[87] Jack Cloherty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad,'" *ABC News,* May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875

[88] Department of Defense Headquarters, Joint Task Force Guantanamo, "Khalid Shaikh Mohammed," *New York Times Guantanamo Docket,* June 2014, http://projects.nytimes.com/guantanamo/detainees/10024-khalid-shaikh-mohammed

[89] "Osama bin Laden trivia: Civil engineer, affluent construction magnate and bomber," *International Business Times,* May 3, 2011, http://www.ibtimes.com/osama-bin-laden-trivia-civil-engineer-affluent-construction-magnate-bomber-282133

[90] Diego Gambetta and Steffen Hertog, "Engineers of Jihad," *University of Oxford Sociology Working Papers,* 2007, http://www.nuff.ox.ac.uk/users/gambetta/engineers%20of%20jihad.pdf +

[91] Ibid.

[92] Hannah Stone, "Mexico Drug Gang Claims Pepsi Subsidiary Helped Govt Agents," *Insight Crime,* June 1, 2012,

series of attacks occurred on Sabritas property, where several distribution centers and 40 company trucks were firebombed. Knights Templar stated that the message was addressed to "all national and transnational businesses," and that they carried out the attack because "intelligence workers and government agents pass themselves off as salespeople in a company."[93] A year later, the cartel moved on to attack power grid infrastructure. In October 2013, Knights Templar attacked electrical plant substations and gas stations in Michoacán, Mexico. Homemade bombs were launched and shots were fired at 18 electrical plants and six gas stations, causing over 420,000 residents to lose electricity.[94] While drug cartels have not posed an imminent threat to the electrical grid in the United States, there is discussion of the potential for these threats, especially along the southern border.

## OTHER GROUPS

While protecting our country's security against international terrorist or insurgent groups is a priority, there are domestic groups that pose a grave threat to the stability of our nation's critical infrastructure. Many groups may seek to act in terms of ecological, anarchical, or anti-capitalist motives in the form of physical threats such as "eco-terrorism" and cyberattacks.

### ECO-TERRORISM

One of the most well-known events of eco-terrorism was in 1989 with the Evan Mecham Eco-Terrorist International Conspiracy (EMETIC), who were arrested following an attempt to destroy a transmission tower near the Palo Verde Nuclear Generating Station in Arizona. [95] This group has had a history of engaging in terrorism against nuclear power plants in the Southwest U.S., as well as damaging infrastructure that negatively impacted the environment. Additionally, the EMETIC was indicted for planning attacks against the Central Arizona Project, the Diablo Canyon Nuclear Facility in California, and the Rocky Flats Nuclear Facility in Colorado.[96]

---

[93] Ibid.
[94] Lizbeth Diaz, "Mexico forces kill two suspects in state energy firm attacks," *Chicago Tribune,* Oct. 28, 2013, http://articles.chicagotribune.com/2013-10-28/news/sns-rt-us-mexico-violence-20131028_1_michoacan-knights-templar-mexico-city
[95] James F. Jarboe, "The Threat of Eco-Terrorism," Testimony before the House Resources Committee, Subcommittee on Forests and Forest Health, *Federal Bureau of Investigation,* Feb. 12, 2012, http://www.insightcrime.org/news-briefs/mexico-drug-gang-claims-pepsi-sub-helped-govt-agents http://www.fbi.gov/news/testimony/the-threat-of-eco-terrorism
[96] Ibid.

Another environmental group known for their acts of eco-terrorism and vandalism is "Earth First!." Although the group has never directly damaged grid infrastructure, due to their history of engaging in unlawful acts to promote their ideology "Earth First!" is considered a major potential threat, as reported by the National Electric Sector Cybersecurity Organization Resource.[97] In addition, both the Earth Liberation Front (ELF) and Animal Liberation Front (ALF) have been known to resort to violence, vandalism, and arson. On December 7, 2005, federal officials arrested six suspected eco-terrorists from ELF and ALF, who claimed responsibility for removing a bolt from a transmission tower in Bend, Oregon, and causing the eighty-foot tower to collapse.[98]

## "HACKTIVISTS"

An additional domestic issue regarding cyber threats is the rise in "hacktivism," or the breaching of computer systems as a form of civil disobedience or to promote political ends such as free speech or non-censorship on the Internet.[99] One of the most pervasive groups, "Anonymous," has been responsible for several cyberattacks, such as releasing the personal information of over 4,000 bank executives on a U.S. government website in addition to claiming responsibility for hacking into credit card companies such as Visa Inc., MasterCard Inc., and eBay Inc.'s PayPal.[100] A splinter faction of Anonymous, "Lulzsec," was the group responsible for hacking into the CIA's public site and exposing personal information.[101]

As of now, groups such as Anonymous and Lulzsec have only attacked corporations and government agencies, typically exposing classified data. Most hacktivists use "botnets," which can control many PCs all at once. The hacker is then able to bombard the system with demands, thus crashing the system and denying public access.[102] Due to the relative ease of these capabilities, hacktivist groups may be able to gain access to crash systems within the power grid. The National Security Agency stated that

---

[97] Bill Gertz, "Inside the Ring: U.S. power grid defenseless from physical and cyber attacks," *Washington Times,* April 16, 2014, http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/?page=all

[98] James M. Taylor, "Six Suspects Arrested for String of Eco-Terrorist Attacks," *Heartland,* February 1, 2006, http://news.heartland.org/newspaper-article/2006/02/01/six-suspects-arrested-string-eco-terrorist-attacks

[99] Peter Ludlow, "WikiLeaks and Hacktivist Culture," *The Nation,* September 15, 2010, http://www.thenation.com/article/154780/wikileaks-and-hacktivist-culture#

[100] LuAnn LaSalle, "Hacktivists make their cause known online while masked in anonymity," *Winnipeg Free Press,* February 13, 2013, http://www.winnipegfreepress.com/wfpfeatured/hacktivists-make-their-causes-known-online-while-masked-in-anonymity-191029271.html

[101] Michael Winter, "Anonymous takes down CIA site, exposes Ala. Personal data," *On Deadline, USA Today,* Febrary 10, 2012, http://content.usatoday.com/communities/ondeadline/post/2012/02/anonymous-cia/1?csp=ip

[102] Ibid.

Anonymous might be able to cause a limited power blackout, and some federal officials believe Anonymous is headed in a more disruptive direction beyond attacking corporations and government websites.

## INDIVIDUALS & "THE INSIDER THREAT"

Major problems can occur when an employee—purposefully or inadvertently—gains access to an infected USB or is able to plant a virus that destroys a system. The threat of this issue is heightened in the case of many decentralized, local power grids accompanied with minimal physical security and detection systems.

An insider may be able to gain access to the physical components of a power station, thus having the ability to cause serious physical damage. Actors posing threats may be disgruntled employees following termination or employees experiencing financial pressures and stress.[103] Job-related stress and unfortunate events can cause employees to exact revenge or open up insider secrets to third-party inquirers.[104] Many of these events are on a situational basis and apply differently to each company; however, business and utilities should prioritize increased security and employee screening.

Individual attacks can have major effects on communities due to dependencies on the power grid. An individual was arrested in Arkansas for a series of attacks on power lines throughout Arkansas. He acted alone, and did not seem to be involved in a larger terrorist organization. On August 21, 2013, a shackle that secured a 500,000-volt electricity line was cut, and over 100 bolts of the support tower were removed.[105] The tower collapsed, causing power lines to be severed by a passing train and leaving the town of Cabot, Arkansas, without power. On September 29, 2013, the Entergy electricity station in Scott, Arkansas, was set on fire, causing over $2 million in damages.[106] The third and final attack occurred in Jacksonville, Arkansas. Two power poles were cut, one of which was then pulled down by a tractor. This attack caused a 115,000-volt transmission line to fall, triggering an outage for 9,000 people.[107]

---

[103] Byron Acohido, "Disgruntled employees, insiders pose big hacking risk," *USA Today*, March 15, 2013, http://www.usatoday.com/story/tech/2013/03/15/insider-threat-matthew-keys-anonymous/1991265/
[104] Ibid
[105] "Arrest made over Arkansas power grid attacks," *CBS News*, October 14, 2013, http://www.cbsnews.com/news/arrest-made-over-arkansas-power-grid-attacks/
[106] Ibid.
[107] Ibid.

Insider threats oftentimes pose a greater risk than outsider attacks. In an FBI and Computer Security Institute joint Computer Crime and Security Survey, 80 percent of enterprises that responded to the survey cited disgruntled or dishonest employees as most likely to attack.[108]

Additionally, 55 percent of enterprises that responded reported unauthorized access by insiders. While security measures have increased over time, insider threat incidents continue to occur. In 2012, Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) was called to a power generation system that had been targeted by an insider threat. An employee was discovered with an infected USB device after he took the device to the IT department. The infected USB left several machines at the power plant subject to the virus. Fortunately, ICS-CERT and the anti-virus software already existing in the system were able to eliminate the virus.[109]

In 2011, the Department of Homeland Security issued a report titled "Insider Threat to Utilities." In this report, they stated that "violent extremists have, in fact, obtained insider positions," and that "outsiders have attempted to solicit utility-sector employees" for damaging physical and cyberattacks.[110] In 2010 an alleged American recruit to al-Qaeda was arrested in Yemen. Sharif Mobley, of New Jersey, had been employed at five different U.S. nuclear power plants in Pennsylvania after successfully passing federal background checks.

Although insider threats to the power grid have been fairly contained, internal security must remain a priority. There should be periodic risk assessment throughout an enterprise, as well as increased security awareness training for employees. Companies can issue strict passwords for employees, monitor online actions, and note suspicious behavior. The company should separate duties and limit access amongst different employees to ensure that one person does not have the ability to cause major damage. Following termination or transfer, any previous computer access must be deactivated. Additionally, up-to-date anti-virus software and backup and recovery processes should be implemented for all online systems.[111]

---

[108] Richard Power, "1999 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends,* 1999, https://www.ncjrs.gov/App/publications/abstract.aspx?ID=177362

[109] "Malware Infections in the Control Environment," *US Department of Homeland Security,* Dec. 2012, http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

[110] "DHS warns utilities at risk from insider threats," *Homeland Security News Wire,* July 25, 2011, http://www.homelandsecuritynewswire.com/dhs-warns-utilities-risk-insider-threats

[111] Dawn Cappelli, Andrew Moore and Timothy Shimeall, "Protecting Against Insider Threat," *Software Engineering Institute,* February 1, 2007, http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200702.cfm.

# SECURING THE GRID

## PHYSICAL SECURITY

Protecting the physical security of the national electrical grid poses a serious challenge. The diffuse nature of the grid makes it exceedingly vulnerable to physical attacks from many angles. Additionally, the networked nature of the grid and reliance on critical nodes means that one small attack or incident has the potential to cause a cascading failure that affects a wide-ranging area. However, the interconnectedness of the grid also allows for redundancies and resiliency within the system.

The energy grid has clear vulnerabilities that can be exploited by those who wish to attack the grid. Much of the electrical grid suffers from decaying and outdated infrastructure. Many of the major components, including transmissions, distributors, generators, and transformers, that make up the grid are over 25 years old, and have undergone minor repairs to patch up issues in the past. According to project participants, in order to replace any damaged parts or update older components, replacements must be manufactured overseas with a 12-15 month lead-time.

This delay in accessibility to new components further highlights the importance of keeping the components up to date before an emergency arises. The majority of stations, transmissions, and distribution lines are located in remote areas above ground, making them easily accessible targets. Transmission systems are especially attractive targets based on their functional importance. Step-up transformers increase voltage so the electricity can flow efficiently over long distances, and step-down transformers reduced voltage for consumption; both of these systems are critical in maintaining voltage levels in a substation to control the general transmission system.[112]

Substations, which often house transformers, are typically only protected by a chain link fence and a few surveillance cameras, both relatively easy to bypass, pinpointing a major lack of physical protection. In April of 2013, a group of people attacked a PG&E Metcalf substation in San Jose, California. The substation was near a highway, and the attackers were able to enter through manholes. They used assault rifles and fired over 100 shots, critically damaging over a dozen transformers.[113] The attack was recorded

---

[112] Knapp, Eric D. , and Raj Samani. "Chapter 2 Smart Grid Network Architecture." In *Applied Cyber Security and the Smart Grid: Implimenting Security Controls into the Modern Power Infrastructure*. : Newnes , 2013. .

[113] Shane Harris, "'Military-Style' Raid on California Power Station Spooks U.S.," Foreign Policy, Dec. 28, 2013, http://complex.foreignpolicy.com/posts/2013/12/24/power-station-military-assault

on surveillance cameras, but the footage proved unhelpful in finding the attackers, and the cameras were clearly unhelpful in deterring the attack.

Transmission components within the grid are regulated by the Federal Energy Regulatory Commission, FERC, and the North American Reliability Corporation, NERC. Following the Metcalf incident, in light of reports raising concerns about the physical security of the grid, NERC discussed new standards for the protection of critical sites and transmission equipment. A major portion of the debate surrounding these standards discussed balancing the need for security with the cost of hardening remote sites or providing round-the-clock surveillance and quick response at grid sites.

These standards, currently being prepared for filing with FERC, require security planning for the bulk power transmission system and updated preparations for physical security.

Distribution systems are regulated on the state level. Multiple regulators may not have the same level of resources for addressing these security issues or communicating concerns to utilities. Additionally, when the issue of cost recovery for security improvements is discussed, these state regulators will be the ones responsible for adjusting rate structures.

It will also be vital for electrical, natural gas, and water utilities to work together with each other and the federal government to expand preparation capabilities, bolster information sharing techniques, stockpile spare equipment, and engage in mutual assistance agreements to ensure a crisis could be handled efficiently.

Electrical grids offer a wide range of targets that can impart a great deal of damage on an entire system. Small-scale attacks can affect much greater systems because the entire grid is interconnected. Project participants warned that once one component is compromised, an entire system could be subject to a cascading failure, thus impacting far more than the initial target.

## GENERATION FACILITIES

Generators and turbines are attractive targets for those who want to maximize the damage of their attacks. Generators and turbines serve as primary power sources for large areas; eliminating the generator cuts power to a vast number of users, thus creating a potentially large-impact power outage.

These two components are also extremely vulnerable to bombings, as they are sensitive pieces of equipment that can be damaged easily. In the wake of an attack, damage done to the generators and turbines would be difficult to repair because they are not easily replaced and spare units are not readily available. Units are expensive and represent a large capital investment for any country, and would raise the cost of any potential conflict that would ensue following the attack. The long lead-time for repair means that heavy damage of components would result in long-term power outages. Other than an entire repair, power would have to be imported from another plant in order to restore the generator.

Generating facilities are attractive targets for those who wish to impact the electrical grid. Generating facilities are at the heart of the energy flow within the grid; they are comprised of turbines and generators that produce the electricity. When force, often from steam or wind, is applied to the blades of a turbine, it causes the generator to rotate which creates the electricity that is dispersed throughout the grid.[114] Both the turbines and the generators are often located in the same building, and, in many cases, the same unit. The turbines' and generators' proximity to one another make it easier for an attacker to target both components at the same time, thus causing an even more dramatic failure.[115] Power interruption can be achieved in several ways at the source. Attacking the buildings that contain the turbines and generators can cause the systems to shut down, therefore interrupting power flow. The components themselves are very delicately balanced and rotated at high rates of speed, making them extremely susceptible to air attacks.

Hydroelectric plants also house generators and turbines, making them another center of power generation. At a hydroelectric plant, attackers may try to destroy the turbine or the generators. A potential bombing or violent attack to the plant would most likely be concentrated in the generator hall. Attackers could also rely on the "fuel," the retained water, to accomplish their goals. In this scenario, there would most likely be an attack on the dam or the penstocks, tubes used to take water from the storage to the turbines, in an attempt to destroy the hydroelectric plant.

Nuclear power plants have become another attractive target. The growth of nuclear power has pushed nuclear power plants higher on the list of potential targets, making them a new and growing problem for targeting by both nation-states and terrorist groups. As of 2012, nuclear power comprised 12.3 percent of the world's energy

---

[114] Griffith, Thomas E. Jr. "Strategic Attack of National Electric Systems." Air University Press. Maxwell Air Force Base, Alabama. October 1994. http://www.comw.org/pda/fulltext/griffith.pdf. Page 5-6.
[115] Ibid.

production.[116] Unlike a hydroelectric plant, interdicting the fuel supply is difficult because only small amounts of fissionable material are used to fuel a nuclear power plant. However, the close proximity of the generator hall and the nuclear reactor make it a more feasible target to attack. Following September 11th, the already tight security at nuclear power plants was increased. However, terrorist groups will still likely pay increased attention to nuclear sites due to the psychological effect of a successful attack—or even an attempted attack—on such a facility.

## TRANSMISSION LINES

Transmission lines are also easily accessible targets, and have the ability to magnify the damage of small attack. Transmission lines deliver power from generators to distribution networks. Once electricity is generated it is sent to a step-up transformer in a substation, or a transformer yard, near a power plant. The step-up transformers increase the voltage of the electricity so it can be transferred long distances along transmission lines. The transmission lines interconnect with generator facilities, thus allowing for the economic exchange of power. They improve the reliability of an entire power system by providing a means of transferring power from one area to another.[117] The transmission system ends at a transformer yard where voltage is reduced through step-down transformers and the electricity is sent through the distribution network for consumers' use. The step-up transformers are the most lucrative targets, because they can impart the most damage with the least effort. Damaging a step-up transformer will disrupt power distribution along many transmission lines, leading to widespread power outages. The Office of Technology Assessment cites step-up transformers as the most vulnerable target with the most consequences throughout the energy grid. [118]

Transmission lines are located in open areas, are easily identifiable, and are not easily interchangeable between systems, also making them vulnerable to attack. Within transmission the electricity's voltage is raised to allow for long distance travel, however, this increased voltage makes the electricity in transmission lines even more dangerous and more able to cause damage to nearby systems or infrastructure than those lines providing energy to homes. In addition to the aforementioned attack on transmission

---

[116] Nuclear Energy Institute. "World Statistics Nuclear Energy Around the World ," http://www.nei.org/Knowledge-Center/Nuclear-Statistics/World-Statistics

[117] Griffith, Thomas E. Jr. "Strategic Attack of National Electric Systems," Page 7.

[118]U.S. Congress, Office of Technology Assessment, *Physical Vulnerability of Electric System to Natural Disasters and Sabotage, OTA-E-453* (Washington, DC: U.S. Government Printing Office, June 1990).

lines in Arkansas, experience in the Middle East has shown that the transmission lines are attractive targets to insurgent groups.

In 2003, a massive blackout affected about 50 million Americans throughout the Northeast and Midwest, as well as customers in Ontario, Canada, displaying the large disruption that can be caused by the failure of transmission lines. In one instance that exacerbated the blackout, the Stuart-Atlanta 345-kV transmission line tripped offline when it sagged into a tree. [119] The loss of this transmission line, along with several others, caused power to be redirected to still functioning lines that were connected. Under the stress of carrying the extra loads, more power lines began to fail, causing a cascading failure. Major cities, such as Albany, Cleveland, Detroit, Hartford, and New York City, experienced widespread electrical failures at over 256 power plants.[120] Crews were unable to restore power for four days in some parts of the United States, and Ontario suffered from rolling blackouts for over a week after the incident.

## SUBSTATIONS & TRANSFORMERS

Step-down transformers could be targeted, but are less attractive targets when compared to generators, turbines, transmission lines, or step-up transformers. The distribution network begins at step-down transformers. They reduce the voltage of the electricity in the transmission lines so it can be distributed for consumer use. Distribution facilities, like transmission lines, would not be attractive targets for air attacks.[121] Step-down transformers are smaller and more difficult to attack than step-up transformers. Multiple distribution systems are supplied from one main power source, which allows the transformers to be more standardized and interchangeable, thus making repairs easier. Any attack would only have a localized impact, not widespread damage. The only potential threat would be to ancillary systems.

To lock down the physical security of the power grid multiple steps must be taken to deter and prevent attackers from entering the system and causing damage. Access to substations and other potential target sites must be heavily secured. In addition to some components themselves, some control systems are located in the power stations that control all the power within the stations; others are physically separated from the system but are still able to control the entire systems remotely.

---

[119] "5. How and Why the Blackout Began in Ohio." *August 14th Blackout Causes and Recommendation*: 45 - 72. http://www.nerc.com/docs/docs/blackout/ch5.pdf (accessed January 1, 2014).
[120] Holgun, Jamie . "Biggest Blackout in US History." *CBS news*, , sec. US.
[121] Griffith, Thomas E. Jr. "Strategic Attack of National Electric Systems." Page 8.

More security surrounding potential targets is crucial; in examining the successful physical attacks on the grid, it is apparent that at some sites, the current system of fences surrounding power stations has proven very easy to maneuver. Beyond the physical fence line, the Metcalf incident showed that standoff attacks can be used to disrupt grid operations without breaching the site perimeter.

Additionally, in securing physical sites, it is important to understand the nexus with cybersecurity measures. In the event of an attack, smooth operation should be in place to transfer power, either by automated computers or manually. Development of new hardware and software for grid control and security can help decrease the grid's vulnerabilities in the future.

If an attack should cripple the grid system, rapid response and warning systems should be in place to alert response teams. The earlier crews are aware of the failure, the less damage can be done, thus avoiding a major crisis. In the 2003 blackout, alarm systems failed on the primary and secondary systems, which contributed to the widespread and long lasting damage that ensued; had the failures been caught earlier, many customers would have been saved from power outages.

## CYBERSECURITY

With the continued use of Supervisory Control and Data Acquisition (SCADA) systems and the installation of Smart Grid technologies, it has become imperative for electrical utilities to harden these systems against a wide range of physical and cyber threats. Throughout the series of roundtables, participants commented on the possibility of a joint cyber and physical attack, which could cripple multiple sectors of critical infrastructure within the country. Before SCADA systems can be fully secured, utilities must also understand its limitations and vulnerabilities, which include "improper input validation; permission, privileges, and access control; and improper authentication."[122]

While hardening these systems in response to threats such as Stuxnet, Flame, and Energetic Bear has proved to be a daunting challenge, it is essential to the safety and security of all electrical utilities and the American people. With the installation of these systems and the development of new hardware and software for grid control, both utilities and consumers have a unique opportunity to gain a greater understanding—

[122] "Cyber Security a Priority to Protect SCADA Systems," Industrial Ethernet Book, 2014, http://www.iebmedia.com/?id=9870&parentid=74&themeid=255&showdetail=true&bb=true

through real-time information flows—about electrical generation, transmission, distribution, and use. Additionally, there is a unique chance to build security into infrastructure as new systems are developed and installed.

## SCADA SYSTEMS & VULNERABILITIES

SCADA systems make up an automated network, which can collect data, analyze data, and generate reports. This network of devices gives utilities the ability to control and measure certain elements within the overall utility system. Early systems date back to the 1920s, but wholesale adoption of SCADA systems by utility operators grew rapidly in the 1960s. By the 1980s, largely standardized SCADA architectures were developed.

SCADA systems are present in all aspects of electric generation, transmission, and distribution. Many electrical utilities install SCADA to perform a variety of functions such as monitoring the operation of circuit breakers, detecting current flows and line voltage, and to take sections of the power grid online or offline. Within the SCADA system itself are a range of components that all work in tandem—Human Machine Interface (HMI), Supervisory System, Remote Terminal Units (RTU), Programmable Logic Controller, and Communications Infrastructure. For example, a RTU can measure or monitor a specific process and send that data back to the main or HMI system for analysis.

Since its inception, SCADA systems have gone through multiple generations of development and the latest generation is described as a networked system. "The major improvements in the third generation [are] that of opening the system architecture, utilizing open standards and protocols and making it possible to distribute SCADA functionality across a WAN [Wide Area Network] and not just a LAN [Local Area Network]." This—combined with improved metering technology, improved consumer interfaces, and additional communications advances—serves as the foundation of Smart Grid technology.

This new generation of SCADA now has the ability to be implemented over a wider range through multiple components connected through communications protocols. This distributed architecture of SCADA now gives utilities the ability to run multiple systems over a wide geographic area but is monitored by a single supervisor. However, the networked nature of this SCADA system does force the utility to focus upon application security, intrusion detection, and the regulation of physical access to the SCADA network.

With these technological developments that have extended the SCADA system's use, it has become more vulnerable to environmental, electronic, cyber, and physical threats. Equipment, such as sensors or actuators, should be properly enclosed to mitigate damage from weather events, such as earthquakes or lightning storms, or corrosive agents. Additionally, operational control rooms should be properly secured from fire or water damage to computers and other equipment. The electronic threats to the SCADA system include radio-frequency interference (RFI), electromagnetic pulse (EMP), and voltage transients. As a result, utilities must properly design infrastructure and can install transient voltage surge suppression (TVSS) to mitigate any damage.

Even though SCADA systems are physically installed in secure locations throughout a utilities' facility, there are a variety of threats that can compromise that security. If an insider or an unauthorized individual gained access to the facility, he or she could use an infected USB stick, disconnect systems, or install a key logger to expose the system.

These threats could infect the system immediately or provide attackers with "back-door" entry to the utility, in which a cyberattack could be used to damage the entire network. Many of the cyber threats include denial of service, data interception, unauthorized user access, data alteration, and/or data-retransmission. Not only could these threats lead to a major blackout for millions of customers, but it could interrupt the ability for other sectors of critical infrastructure to function or allow highly sensitive material to be obtained. Securing against such challenges not only requires the development of improved security protocols for utility employees, but also improved behavioral analysis aimed at preventing or detecting unauthorized access or software installation—be it inadvertent or malicious.

## DETERRING & DETECTING ATTACKS

Electrical utilities and other critical infrastructure facilities must begin to implement various practices and methodologies that can secure SCADA systems from these threats. Utilities have begun to integrate Software Management and Documentation Systems (SMDS) into SCADA, which monitor all of the activities of the control system. SMDS can assist IT and OT operators with an application restoration following a catastrophic event; control who may use any SCADA application system; and can control which actions can be performed. Additionally, many utilities have begun to develop various Network Security Solutions, which range from firewalls to "Demilitarized Zones" to physical "air-gaps," which prevent unwanted access to a network.

Through the use of a Virtual Private Network tunnel (VPN) utilities can ensure the proper authentication and authorization of data transactions between different networks. VPN gives a utility private use of a public network through the development of an encrypted tunnel between the server and client. To remain secure, when logging onto the VPN, the secondary device must have the same level of end-point protection; if there is a variation, it can create vulnerabilities to the VPN. To fully secure the VPN from unauthorized access, a high level of authentication must be implemented in all networked devices.

Due to the high amount of threats to SCADA systems, utilities have also begun to implement detection methodologies to mitigate the effect of an attack. IT security systems have created Intrusion Detection Systems (IDS) which are designed to recognize intrusions based upon multiple factors including an unusual pattern of activity and communications attempted from an unusual or unauthorized address. The IDS creates a log of suspicious events, which system operators can inspect manually to determine true intrusions versus false alarms. Through the implementation of IDS, OT personnel have the ability to use firewalls to prevent the attack from spreading, thus mitigating the overall damage the cyber threat could cause.

In addition to technological solutions, securing networks will require an increased emphasis on behavioral analysis, background investigations, psychological profiling, and analysis of individual motives. These factors are key tools for detecting potential insider threats, while also revealing how potential adversaries may seek to target individuals who can provide access—purposefully or inadvertently—to vital networks.

## TYPES OF CYBERATTACK

As threat actors are becoming more advanced, the attacks perpetrated against computer systems are increasing in frequency, intensity, and variety. Various types of attacks such as data interception, denial of service (DDoS), data alteration, or a cyber "drive by shooting," have been utilized by groups, individuals, or nation-states depending upon their strategic objective.

Many of the viruses that have caused substantial damage to critical facilities across the world were specifically designed to compromise SCADA systems. The Stuxnet virus, which was discovered in June 2010 in Iran, infected over 100,000 computer systems throughout the globe. This virus contained specific code that was designed to attack the Siemens Simatic WinCC SCADA systems by intercepting commands from HMI

software. Stuxnet intercepts commands sent to high-speed frequency converters, which are devices that control functions, such as motors.

Additionally the Flame virus, which was discovered in May of 2012, also compromised Iranian SCADA systems through cyber sabotage. The malware monitored and mapped out the country's computer networks through the replication of controls and daily tasks associated with HMI functions. Flame has the ability to log keyboard stokes, take screen shots, activate microphones and cameras, and receive and send commands and data through Bluetooth wireless technology. These two viruses, which were directed towards Iranian nuclear facilities and other high-profile computer networks, demonstrate the potential of sophisticated cyber threats tailored to target SCADA systems.

In the spring of 2014, the Heartbleed Bug was found to be a security vulnerability within OpenSSL software, and had infected over 500,000 websites, including Yahoo and OKCupid. This flaw let hackers access the memory of data servers, leaving personal data such as passwords, credit card information, and usernames vulnerable. A Secure Sockets Layer, or Transport Security Layer, is the most basic "encryption standard [widely] used by websites that need to transmit the data that users want to keep secure."[123] On occasion, a computer will check if there is another computer at the end of its secure connection by sending a small package of data, a "heartbeat," that requests a response. Due to a "programming error in the implementation of OpenSSL, the researchers found that it was possible to send a well-disguised packet of data that looked like one of these heartbeats to trick the computer at the other end into sending data stores in its memory."[124]

A researcher at Google and the security firm Codenomicon discovered the flaw in OpenSSL and confirmed that the bug had been active for at least two years. Due to the highly sophisticated nature of the bug, hackers were able to steal encryption keys used by websites to secure personal information. Additionally, the Heartbleed Bug demonstrated how vulnerabilities in the basic architecture of the Internet can be exploited by hackers.

Most recently, electrical grid infrastructure within the United States and Europe has come under attack from a group of Russian hackers known as "Dragonfly." Since 2011, the group has been conducting various cyberattacks, typically classified as espionage,

---

[123] Kyle Russell, "Here's How to Protect Yourself from the Massive Security Flaw That's Taken Over the Internet," *Business Insider,* April 8 2014, http://www.businessinsider.com/heartbleed-bug-explainer-2014-4

[124] *Ibid*

against European governments, defense contractors, and U.S. health care firms. Although, as of late, Dragonfly has been conducting Stuxnet-type attacks against the industrial control systems found with petroleum pipeline operators, grid operators, electricity generation firms and other critical energy companies.[125]

Dragonfly has developed two Remote Access Trojans (RAT) to install malware on computers, which gives hackers access and control over the infected computer. These attacks, referred to as "Energetic Bear," "are centered on extracting and uploading stolen data, installing further malware onto systems, and running executable files on infected computers…[and] running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloguing documents on infected computers."[126] In addition to the RATs, the group has utilized other attack vectors such as spear phishing/email span, watering hole attacks/exploit kits, and other trojanized software to destroy the integrity of specific systems. Although the exact motivation for these attacks is unknown, multiple researchers have stated that the RATs utilized by Dragonfly are too advanced and the attacks "bear the hallmarks of a state-sponsored operation."[127]

## THE NEED FOR RAPID INFORMATION SHARING

Currently there is agreement that information sharing channels between the government and the private sector and amongst private sector firms are necessary to improve risk assessment, situational awareness, and increase the overall security of the electrical grid. Regardless of the differing models as to how this might be implemented—e.g. coordination centers, third-party operators, public-private partnerships—these structures will implement methods of real-time sharing of private, proprietary, or classified information. In the absence of cybersecurity legislation, many of the current practices have yet to be codified into law, increasing concerns regarding privacy and liability.

Even with the recent statement released by the FTC and DOJ, there are still questions concerning the ability to provide liability protection for the private sector to ensure that sharing information about a threat or vulnerability does not, in turn, leave a company

---

[125] Amy Thomson & Cornelius Rahn, " Russian Hackers Threaten Power Companies, Researchers Say," *Bloomberg,* July 1, 2014, http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms.html

[126] "Emerging Threat: Dragonfly/Energetic Bear – APT Group," *Symantec,* June 30, 2014, http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group

[127] Ibid.

vulnerable to legal or regulatory penalties. In addition to fostering information sharing between private sector entities, continued assurances are needed so that such information exchange is not viewed as collusion by antitrust regulators.

Additionally, problems regarding the information sharing process have centered upon the high volume of classified information sent to utilities. An important aspect of vertical information sharing focuses on developing a "tear line" in which utility operators have the necessary information about a cyber or physical threat. By developing a more practical tear line, a wider range of personnel throughout a utility will have access to information, which could help deter, mitigate, and respond to an attack.

Considering that multiple governmental agencies disseminate information to utilities—including the DOE, DHS, DOD, FBI, and the Intelligence Community—many of the grid operators are inundated with information. As a result, the federal government should implement practices that will focus upon sending the most critical of information to utilities. This could be achieved through integrating federal government personnel in the private sector to better understand what threat information is necessary and useful to utilities. Additionally, some of the most imperative information to be shared regarding a cyberattack is a threat signature, which is a unique string of bits or the binary pattern of a virus. Simply put, a threat signature is similar to a fingerprint, which can be used to detect and identify specific viruses.[128]

Not only is an active defense towards deterring cyberattacks imperative, but also utilities must utilize the current forums for sharing information, such as the Information Sharing Action Center (ISACs), the Electricity Sub-Sector Coordinating Council (ESCC), and the National Cybersecurity and Communications Integration Center (NCCIC) at DHS. By using these bodies, electrical utilities across the country have the ability to share alerts, indicators, information about previous attacks, threat actors, and threat signatures.

Through the ISACs and ESCC, owners and operators throughout the electricity sector have the ability to share information regarding threats and attacks that are both cyber and physical in nature. Not only can members of the industry coordinate policy to improve resilience and reliability, but this information is sent to the appropriate channels within the federal government. It is extremely important that utilities utilize these information sharing bodies and Mutual Assistance Agreements (MAAs) in the wake of an event, such as Superstorm Sandy or Metcalf. For example, if a utility

[128] "McAfee Threat Glossary," *McAfee*, 2014, http://www.mcafee.com/us/threat-center/resources/threat-glossary.aspx

needed to shift a load to keep the lights on or obtain a spare transformer, they could go through the ISAC, ESCC, or MAA.

While Mutual Assistance Agreements are well practiced and have a strong historical track record, there are many questions surrounding the structure and efficacy of MAAs in light of a cyber-incident that would require computer hardware, software patching, or coding expertise, for example, rather than the herculean efforts of lineman replacing damaged transformers.

At the federal level, multiple agencies monitor the status of critical infrastructure including the National Cybersecurity and Communications Integration Center (NCCIC) at DHS. The NCCIC works with entities at the federal, state and local levels, including law enforcement, to prepare, mitigate, and respond to cyber threats.[129] Through horizontal and vertical sharing, utilities will be able to develop an "integrated response plan" to an attack through more informed decision-making.[130]

## ADVANCES IN HARDWARE & SOFTWARE

Due to an increased volume in data from Smart Grid technology, utilities must find methods to analyze it all in real-time. Additionally, on an organizational level, "siloed utility operations must share data and analytic resources, to avoid wasting time and money on duplicative and isolated efforts." Companies such as GE, Siemens, Oracle, AutoGrid, Trove, IBM, and SAS have all begun to develop data analytic software. The three most widely implemented grid analytics solutions are voltage optimization, asset management, and outage management. As information is analyzed in real-time, OT and IT personnel have greater situational awareness to be able to detect and correct problems within the grid.

Similar to aspects of the Smart Grid technology, utilities have begun to implement software to monitor the status of the grid. For example, Powerlogic ION EEM software gives utilities the ability to conduct wide-area analysis of conditions through the application of analytics. "These can include power monitoring and control systems, metering systems, substation automatic and SCADA systems…data is automatically acquired, cleansed and warehoused." Through the application of analytics and grid

[129] "Electric Power Industry Initiatives to Protect the Nation's Grid from Cyber Threats," Edison Electric Institute, Jan. 2013, www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf
[130] "Preparing Utilities to Respond to Cyberattacks," The Wall Street Journal: Deloitte Insights, Jan. 16, 2014, http://deloitte.wsj.com/riskandcompliance/2014/01/16/preparing-utilities-to-respond-to-cyberattacks/

monitoring software, utilities can manage risks, increase efficiency, and in turn, increase reliability.

In terms of physical hardware, systems under development by companies, such as One Cycle Control, allow for automatic adjustment of grid voltage and load. While these technologies have been developed to automatically balance the input of solar and wind generation, they could also work in the event of malicious activity to balance electric power loads. These systems can be designed to work without computerized input, so that in the event of a cyberattack, there could still be an automated, hardware-based response.

As these systems analyze the patterns of grid usage and data access, they can provide a better baseline of activity for the detection of malicious activity. Being able to rapidly identify network or grid behavior that rises "above the noise level" will allow grid operators to quickly isolate affected systems. Doing so requires significant investments in computing power, as well as human operators to understand and analyze the data.

The ideal system would respond with an instantaneous and automated isolation of an affected system and would subsequently reroute network traffic and electric power to minimize disruption. In order for such systems to effectively operate, machine-to-machine sharing of information and threat signatures must be facilitated.

## THE SMART GRID CHALLENGES & OPPORTUNITIES

With the increased use of Smart Grid technologies—e.g. "smart meters" and connected appliances—there is a proliferation of access points into the networks that control grid systems. While previous systems were designed to be easily air-gapped, thus preventing any connection between grid control systems and the public Internet, the design of these systems, and their intended convenience, requires some level of connectivity between utility systems, home systems, and personal devices.

While a utility provider can take steps to secure the hardware and software that runs advanced SCADA systems, smart meters, and other utility-installed systems, the future portends a proliferation of commercial and household devices that will connect to utility systems. Utilities, the manufacturers of these devices, and consumers will share responsibility for ensuring the security of these devices and their connection to the grid. For example, car companies will play a significant role in grid security, as electric cars or plug-in hybrids will connect to the grid and either draw or return power based on grid demand.

Such devices and future advancements in technology provide the opportunity for increased efficiency, smarter consumption, and better situational awareness, but the looming security challenges will require increased attention as well.

## ELECTROMAGNETIC PULSE, DIRECTED ENERGY & GEOMAGNETIC STORM

In addition to physical and cyber threats that endanger the security of the electrical grid, electromagnetic pulse (EMP), directed energy weapons (DEW), and geomagnetic-induced currents (GIC) could also the damage the grid. These "high-impact, low frequency" risks have continued to become more dangerous, as American society increasingly relies upon computerized electronics in key sectors, such as telecoms, financial services, and other critical sectors, alongside vital government functions, such as the military and emergency services.

As discussed within the roundtables, one of the most essential aspects to securing the electrical grid against these threats is to strengthen communication between utilities and the federal government in order to improve the science about EMP, GIC, and DEW, and to harden key grid nodes and facilities. Through this partnership, both sides can work to implement the best practices and 21st century technology to mitigate the effects of EMP, GIC, or DEW.

### ELECTROMAGNETIC PULSE

One of the more significant threats to the security of this nation's electrical grid is that of electromagnetic pulse (EMP). Yet there are many outstanding questions about the scope and effects of EMP, as well as a limited number of actors capable of launching such an attack. Unlike the other threats described in this report—with the exception of a major cyberattack launched by another nation-state—the detonation of an EMP over the United States would be a clear act of war, and many of the preparations and responses are questions of broader national security rather than grid security. Still, as nuclear and missile technology continue to proliferate, EMP will continue to be a concern for security planners.

Simply put, EMP is an "intense energy field that can instantly overload or disrupt numerous electrical circuits at a distance."[131] Historically, there have only been a few recorded instances of EMP damaging electrical grid infrastructure. In 1962, the United States conducted the *Starfish Prime* 1.4-megaton nuclear test approximately 20 miles from Johnston Island in the Pacific Ocean. The explosion, which occurred at an altitude of 250 miles, affected electronic equipment almost 800 miles away in Hawaii. Also occurring in 1962, the Soviet Union conducted the K-3 nuclear test, which was a 300-kiloton blast at 180 miles altitude. Not only did the test result in significant phone line and power disruption, but a fire destroyed a power plant in Kazakh SSR.[132] Since the creation of the Limited Test Ban Treaty, international law has prohibited the testing of nuclear weapons under water, in the atmosphere, or in space. As a result, there has been very little development in the knowledge about the scope and range of EMP related damage.

EMP can be classified into three different types: Lightning Electromagnetic Pulse (LEMP), Electrostatic Discharge (ED), and man-man EMP, specifically High-Altitude Nuclear Electromagnetic Pulse (HEMP) and Non-Nuclear Electromagnetic Pulse (NNEMP). With the proliferation of fissile material and rouge states continuing to develop nuclear weapons, a HEMP attack would be the most devastating to all aspects of American society.

HEMP is "an electromagnetic field produced in the atmosphere by the power and radiation of a nuclear explosion."[133] An intercontinental ballistic missile or a high altitude missile equipped with a nuclear warhead could achieve HEMP when detonated 15 miles or more over the Earth's surface. The nuclear explosion itself would not damage infrastructure, but the three energy components that comprise HEMP has the ability to overload computer circuitry.

The first energy component of HEMP "is the initial shockwave which lasts about one microsecond, and is similar to extremely intense static electricity that can overload circuitry for every electronic device that is within line of sight of the burst. The second energy component…has the characteristics that are similar to a lighting strike… [and] the third energy component is a longer-lasting magnetic signal…[which] causes an effect that is damaging primarily to long-lines electronic equipment."[134]

---

[131] Clay Wilson, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment," *Congressional Research Service Report for Congress,* Aug. 20, 2004, http://www.history.navy.mil/library/online/hemp_hpm.htm
[132] Ibid.
[133] Ibid.
[134] Ibid.

The energy field created by HEMP can be picked up by metallic power cables or wires, which function as an antenna and conduct the shockwave into the electronic systems of airplanes, cars, and communications equipment. The three energy components of HEMP damage the electrical grid through the creation of a "localized magnetic effect [which] builds up throughout the length of transmission lines and then quickly collapses, producing a magnetohydrodynamic (MHD) 'heave,' or 'late-time,' power surge that overloads equipment connected to the power and telecommunications infrastructure."[135] The combination of the three energy components of HEMP causes changes in the Earth's magnetic field, which couple with electronic equipment and produce a damaging current and voltage surges. The immediate effects caused by a HEMP attack have the ability to cause a cascading failure throughout large sections of the grid. Due to the nature of this attack, securing the grid from EMP should not just focus upon the ability of utilities to provide electricity to customers but also as a component of broader U.S. national security.

## THE EMP COMMISSION

Due to concerns about EMP, Congress formed the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack in 2003 to "examine the impact of nuclear weapon generated electromagnetic pulse (EMP) on the United States."[136] Its main goals was to assess the capabilities of possible threat actors, determine what aspects of civilian and military systems are highly vulnerable to EMP, evaluate the ability for the country to recover and repair from an attack, examine the cost and probability of hardening systems to mitigate EMP damage, and recommend specific steps the country should take to harden military and civilian systems. Additionally, the EMP Commission brought much needed political and public attention to the issue of electromagnetic pulse—be it manmade or naturally occurring.

In July of 2004, the EMP Commission presented the "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack" to Congress. Not only did the executive report describe the components of EMP itself, but recommended certain steps the country could take to harden critical infrastructure. The EMP Commission further recommended that DHS have the authority to obtain resources, develop plans, and implement strategies that could secure the most critical

---

[135] Ibid.

[136] William A. Radasky, "High-altitude Electromagnetic Pulse (HEMP): A Threat to Our Way of Life," *Todaysengineer.org,* September 2007, http://www.todaysengineer.org/2007/sep/hemp.asp

components within civilian and military systems. Additionally, the report suggested that the US continue to deter terrorist groups and rogue states from developing nuclear weapons capabilities.[137] Ultimately, the EMP Commission concluded that an EMP attack is a grave threat against the country and could cripple multiple sectors of critical infrastructure; the commission's findings indicated that little had been done to secure infrastructure from a possible attack.

As a result, the EMP Commission decided to reconvene in 2007 to evaluate the progress the nation had made in securing critical sectors from an attack. In the 2008 "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," the Commission noted that it was difficult to determine the level of security that had been implemented because an attack had not occurred. This report expanded upon the 2004 report by examining the current status and providing recommendations to secure a variety of sectors including telecommunications, electric power infrastructure, banking and finance, SCADA systems, transportation infrastructure, water supply infrastructure, emergency services, fuel and energy infrastructure, and space systems.

Ultimately, the EMP Commission demonstrated the grave impact that a High-Altitude Nuclear Electromagnetic Pulse (HEMP) attack could have upon civilian and military systems throughout the country.

## DIRECTED ENERGY WEAPONS

Directed Energy Weapons (DEW) are systems or platforms that create EMP-type energy pulse on a smaller and non-nuclear scale. Conventional weapons use the kinetic or chemical energy of a projectile, but DEW can hit the intended target with subatomic particles or electromagnetic waves, which travel at the speed of light. Simply put, DEW use a certain frequency within "the electromagnetic spectrum (light and radio energy) to attack" a specified target.[138]

As a result, there is a large variety of weapons that threat actors can develop depending upon the intended outcome of an attack. Lasers are the most developed type of DEW and can "form intense beams of light that can precisely aimed across

---

[137] "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Volume 1: Executive Report," *EMP Commission,* July 2004, http://www.empcommission.org/docs/empc_exec_rpt.pdf

[138] Andrew Gudgel & Alane Kochems , "The Viability of Directed-Energy Weapons," *The Heritage Foundation,* April 28, 2006, http://www.heritage.org/research/reports/2006/04/the-viability-of-directed-energy-weapons

many kilometers to disable a wide range of targets: from satellites to missiles and aircraft to ground vehicles."[139] The majority of the Directed Energy technology is currently being developed by the U.S. military, yet there are many other applications for this technology.

Threat actors could utilize DEW to attack certain sections of the electrical grid. For example, modern electronics and semiconductors are extremely vulnerable to High-Powered Microwave (HPM) devices. Not only is the infrastructure of the electrical grid aging, but due to its reliance upon electrical equipment and highly networked SCADA systems, HPM or DEW attacks could cause wide spread blackouts or even a cascading failure.

## TRANSIENT ELECTROMAGNETIC DEVICE & HIGH-POWER MICROWAVE

Two specific types of weapons that have the ability to generate electromagnetic pulse are Transient Electromagnetic Devices (TED) and High-Powered Microwave (HPM) devices. Both of these types of weapons are non-nuclear in nature, which gives more types of threat actors the ability to obtain the materials necessary to develop these weapons. TED and HPM effect and destroy electronic systems in a similar fashion to HEMP, making these weapons a feasible alternative.

Transient Electromagnetic Devices create a "very brief, very high voltage discharge that can momentarily break, and perhaps irreparably damage the functionality of sensitive electronic circuits, memory, CPUs and various semiconductors."[140] The electrostatic radiation that is generated by TED operates on a wideband frequency, which allows the weapon to attack any weak spot within the targeted device.

Considering that these devices can operate on a large spectrum, TED can be configured according to how a threat actor wanted to perpetuate an attack. The most common forms of TED can be designed are "a briefcase-sized device that would be placed in close proximity to the target; a device that could fit into a small van; a not-so-disguised device that would be intended for use in a more remote location; [and] a device 'that could be located in one's backyard such that it could be aimed at

---

[139] James Jay Carafano, Ph. D. & Jack Spencer, "The Use of Directed-Energy Weapons to Protect Critical Infrastructure," *The Heritage Foundation,* August 2, 2004, http://www.heritage.org/research/reports/2004/08/the-use-of-directed-energy-weapons-to-protect-critical-infrastructure

[140] Michael B. Hayden, "Electromagnetic Attackyou're your Infrastructure and Data at Risk?" *Indiana University of Pennsylvania,* August 10, 2001, http://www.lib.iup.edu/comscisec/SANSpapers/hayden.htm

overflying aircraft' to damage airborne systems."[141] Currently, threat actors have the capabilities, both monetary and technologically, to build a Transient Electromagnetic Device that could damage key computerized systems within an electrical utility facility.

Threat actors also have the capability of utilizing microwaves, which is electromagnetic energy that can be used at a moderate power level for radar and radio frequency communications. High-Powered Microwave weapons "generate an intense 'blast' of electromagnetic waves in the microwave frequency band," and have also been referred to as "e-bombs."[142] Threat actors have the ability to develop an e-bomb in multiple ways: the first method utilizes a "power chemical detonation [that] is transformed through a special coil device, called a flux compression generator;" and the second method is through the combination of "reactive chemicals or power batteries" which generates an intense electromagnetic pulse.[143] Additionally, threat actors can attach an antenna or emitter, which can radiate the microwaves over a large area.

HPM weapons are effective due to the types of materials that are utilized when developing electronic equipment. Metallic conductors, found within bipolar devices and metal-semiconductors, absorb microwaves, which causes the material to melt.[144] Due to the nature of the weapon, HPM devices interfere with radio frequency links, which could disable aspects of the electrical grid and telecommunications. Additionally, HPM has the ability to immobilize vehicles that use modern electronic control and ignition systems, thus hindering a utility company's response during a crisis. Ultimately, through the use of TED or HPM, a threat actor would have the ability to target certain electrical equipment at utility facilities, which would disrupt the ability for the grid to function.

## GEOMAGNETIC STORMS

In addition to the manmade EMP threats that endanger the security and stability of the electrical grid, utilities must also physically harden infrastructure against geomagnetic storms. These storms are bursts of energy produced by the sun during a CME, which is

---

[141] "Improvised Electromagnetic Pulse Devices: Possibilities and Realities," http://www.defensemedianetwork.com/stories/improvised-electromagnetic-pulse-devices-2/

[142] Michael Abrams, "The Dawn of the E-Bomb," *IEEE Spectrum,* Oct. 31, 2003, http://spectrum.ieee.org/biomedical/devices/the-dawn-of-the-ebomb

[143] Clay Wilson, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment," *CRS Report for Congress,* July 21, 2008, http://www.fas.org/sgp/crs/natsec/RL32544.pdf

[144] Michael Abrams, "The Dawn of the E-Bomb," *IEEE Spectrum,* Oct. 31, 2003, http://spectrum.ieee.org/biomedical/devices/the-dawn-of-the-ebomb

an occurrence related to a solar flare. The wind plasma that is released during a CME connects with the Earth's magnetosphere, causing various changes in the configuration of the planet's magnetic field. This produces GICs, which have the ability to overload electric transformers and power stations.[145]

One of the largest geomagnetic storms occurred in March of 1989 and led to the collapse of the Hydro-Québec system and the Québec interconnection. A massive blackout in a matter of minutes that affected six million customers was the result. GICs affected protective systems on VAR compensators and generator step-up transformers, and permanent damage occurred to a generator step-up transformer at a nuclear station in New Jersey.[146]

Since 1989, the country has not experienced a geomagnetic storm on that level, yet with technological advancements, the electrical grid is actually more vulnerable. The greatest vulnerabilities are found within transformers and transmission lines, because the higher the voltage rating of a network, the lower its resistance to geomagnetic-induced currents. High-voltage networks have increased from 100-200 kV during the 1950s, to the 345-765-kV extra-high voltage threshold of today. Ultimately, "the ratio of resistance varies significantly with voltage class, as the resistance is approximately 10 times lower for the 765-kV then for the 115-kV lines."[147] Additionally, geomagnetic-induced currents can cause internal heating of transformers, which can lead to saturation of the magnetic core. This damage to the transformer cannot be fixed by utility personnel and, as a result, a new transformer must be obtained. Not only is this process time consuming and expensive, but it hinders the ability of utility and emergency workers to properly and sufficiently respond to an event.

Currently, NOAA and NASA monitor solar weather through the Space Weather Prediction Center with multiple satellites, including the Advanced Composition Explored (ACE) and the Solar and Heliospheric Observatory (SOHO). These satellites are equipped with technology, such as a flux-gate magnetometer or Faraday cup, which measures various aspects of solar weather. "The [Faraday cup] scoops up protons and measures the particles' velocity, temperature and density. Meanwhile, the

---

[145] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," *NERC*, June 2010, http://www.nerc.com/pa/CI/Resources/Documents/HILF_Report.pdf

[146] "Solar Storm Risk to the North American Electric Grid," *Lloyd's and the Atmospheric & Environmental Research, Inc,* 2013, www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/solar%20storm%20risk%20to%20the%20north%20american%20electric%20grid.pdf

[147] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," *NERC*, June 2010, http://www.nerc.com/pa/CI/Resources/Documents/HILF_Report.pdf

magnetometer determines the vector of the solar magnetic field."[148] The measurements taken by the satellites are sent to NOAA's Space Weather Prediction Center in which an automated process analyzes the data and turns it into actionable information. The information obtained by electrical utilities can be used to prepare for an incoming geomagnetic storm.

The Space Weather Prediction Center has categorized the impact of these storms on a scale of G1 to G5, but it is the G4-and-G5-level storms that would have the most significant impact on electrical grid operations. For example, a G3 storm would trigger some automated voltage alarm systems, while a G4 storm would cause some protective systems to mistakenly trip and a G5 storm could cause blackouts and/or transformer damage.[149] Advanced warning from NASA and NOAA could allow utilities to plan for the impact of the storm.

Yet even with advanced warning, utilities are limited in their ability to quickly harden the grid in the advance of a geomagnetic storm. Additionally, many researchers have predicted that if a geomagnetic storm at the level of the Carrington Event were to occur, it could take between four to ten years to recover and could cost between $1 trillion to $2 trillion in the first year alone.[150] As a result, it is imperative that electrical utilities take protective measures to limit the length and scale of a possible blackout.

These measures, similar to the ones taken before an extreme weather event, can range from shifting loads to increasing the power production of alternative energy sources. Additionally, there are several steps utilities can take to physically harden the grid, from Faraday cages to neutral-current-blocking capacitors, which block geomagnetic-induced currents from flowing into at-risk transformers.

The outstanding question in preparing for a GIC event is the baseline standard for preparedness—i.e. for what strength of storm should utilities prepare? While an event like the Carrington Storm would be high-impact, the probability is considered low. Additionally, steps taken to prepare for a lower-impact event could help to mitigate the effects of a higher-impact event, while also allowing for a more even distribution in the costs of hardening the grid.

---

[148] "Solar Storm Risk to the North American Electrical Grid," *Lloyd's and the Atmospheric & Environmental Research. Inc, 2013,* http://spectrum.ieee.org/energy/policy/protecting-the-power-grid-from-solar-storms

[149] "NOAA Space Weather Scales." April 7, 2011. http://www.swpc.noaa.gov/NOAAscales/NOAAscales.pdf

[150] Jay R. Thompson, "The Dangers of Solar Storms: That Which Gives Power Can Also Take it Away," *Earth Magazine*, January 21, 2013, http://www.earthmagazine.org/article/dangers-solar-storms-which-gives-power-can-also-take-it-away

Continued support for the solar observation mission as well as continued study of solar weather and its impact on Earth will be necessary for predicting GIC events and understanding their potential impact on current and future electrical grid technology.

## THE FUTURE

During the roundtables, participants discussed the application of Directed Energy Weapons as a tool for threat actors to use against the U.S. electrical grid. Although this is only one application of DEW, DOD, in tandem with national laboratories, has been developing this technology as a way to advance the armed forces into the 21st century.

Since the Cold War, the United States has been developing particle-beam weapons, and are close to deploying the Tactical High-Energy Laser (THEL) and the Airborne Laser (AL). These new weapons show promise as the THEL became the first system to successfully shoot down a live warhead mid-flight during a test in 2000.[151] In addition to the laser systems, the military has been developing Active Denial Technology (ADT), which is "a non-lethal way to use millimeter-wave electromagnetic energy to stop, deter, and turn back an advancing adversary."[152] The ADT causes severe pain or a burning sensation to an enemy, which in theory, would make them flee the scene. The ADT was tested at Kirtland Air Force Base in 2000 and a prototype was mounted on a Humvee and tested in 2005. After testing, the U.S. Army requested the ADT to use in Iraq, and there are conflicting reports that the technology was used in Afghanistan.

Meanwhile, the U.S. Navy views DEW as an opportunity to revolutionize naval warfare by giving sailors the ability to shoot down 'asymmetric threats' such as aerial drones or advanced missiles. Officials commented that some of the advantages to developing DEW include "less collateral damage, more affordability, less sustainment cost, temporary and reversible effects on targets in addition to limitless magazines compared to kinetic projectiles and very low cost-per-engagement."[153] One of the main DEW programs was the ONR Quick Reaction Capability program, in which scientists and engineers from the Navy were working with individuals from BAE Systems, Raytheon, and Northrop Grumman. That program produced the Laser

---

[151] Alane Kochems & Andrew Gudgel, "The Viability of Directed-Energy Weapons," *The Heritage Foundation*, April 2006, http://www.heritage.org/research/reports/2006/04/the-viability-of-directed-energy-weapons

[152] Leonard David, "E-Weapons: Directed Energy Warfare in the 21st Century," *Space.com*, January 2006, http://www.space.com/1934-weapons-directed-energy-warfare-21st-century.html

[153] "New Naval Directed Energy Center to Impact Future Weapons for Naval and Joint Forces," *NAVSEA*, September 2014, http://www.navsea.navy.mil/nswc/dahlgren/NEWS/directed_energy/directed_energy.aspx

Weapons System (LaWS) prototype, which is scheduled to be installed on the USS *Ponce* for sea-testing in 2014.[154]

## MITIGATION

Currently, the full effects of HEMP, HPM, and DEW attacks are largely unknown. Given that the U.S. is unable to test nuclear weapons and DEW devices are still being developed and tested, scientists have relied upon complex simulations to understand the possible scope of damage from these threats. As a result, there continue to be advances in both offensive and defensive capabilities.

Considering the scope of damage that could be cause by one of these attacks, utilities should focus on hardening key components sections of the grid that could mitigate the overall amount of possible damage in terms of both grid operations and the impact on other critical infrastructures or facilities. Examples include the installation of Faraday cages, surge protectors, optical fiber cables, black-starting capabilities, and motor-generator power isolators, and the use of techniques such as shielding, islanding, or grounding.

Additionally, through the application of new distributed generation techniques, such as a microgrid, emergency services or essential agencies can retain power in the wake of an attack.

Ultimately, the likelihood of these attacks is remote, yet in worst-case scenarios, there would be widespread, catastrophic impacts. While many of these scenarios may appear as if they came from the pages of a science fiction novel, these threats must be understood within the context in which they would occur. Any EMP that resulted from a high altitude nuclear detonation would be a direct act of war against the United States. A massive solar storm would be an unparalleled "act of god." In planning for such an event, it is important to focus on how the grid can absorb the force of the incident, how vital installations can continue to receive power, and how the grid—and society— can quickly bounce back.

---

[154] "All Systems Go: Navy's Laser Weapon Ready for Summer Deployment," *Navy,* April 2014,http://www.navy.mil/submit/display.asp?story_id=80172

## SEVERE WEATHER

While sharing many of the same vulnerabilities as those discussed in terms of physical security, extreme weather events are one of the most significant and regularly occurring threats to grid security. These events, due to climate change, development patterns, and demographic trends, have increased in frequency, intensity, and scope—both in terms of geographic footprint and the size of the populations affected. Typically, inclement weather has the greatest amount of advanced warning and utility operators have the greatest level of experience in preparation and response for these incidents.

Throughout the past decade, the intensity and frequency of extreme weather events have increased resulting in storms such as the 2012 Ohio Valley & Mid-Atlantic Derecho and Superstorm Sandy, which damaged large sections of the electrical grid. In the 2013 Executive Office of the President Report, "Economic Benefits of Increasing Electrical Grid Resilience to Weather Outages," it was estimated that 58 percent of the blackouts since 2002 have been caused by events such as hurricanes, blizzards, and thunderstorms. The large amount of damage to the grid, estimated to range from $18-33 billion, is influenced by the sectors' failing infrastructure and outdated practices.[155] The American Society of Civil Engineers describes the grid as a "patchwork system" that is in desperate need of investment. Recently, ASCE has estimated that $673 billion is necessary to sufficiently update the entire grid by 2020.[156] The amount of damage recent storms have caused indicates both a trend towards severer weather events, as well as the need for grid modernization.

Historically, North America has been experiencing an increase in devastating storms over the past three decades, demonstrated between by the period from 2004-2012 where seven out of ten of the costliest storms in U.S. history occurred. These extreme weather events, nicknamed "billion dollar storms," have been occurring more frequently due to changes in temperature, precipitation patterns, and sea levels. Two of the most recent billion dollar storms are the 2012 Ohio Valley & Mid-Atlantic Derecho and Superstorm Sandy.

---

[155] Clare Foran, "Climate Change is Threatening the Power Grid," *National Journal,* Aug. 12, 2013, http://www.nationaljournal.com/energy/climate-change-is-threatening-the-power-grid-20130812

[156] Richard J. Campbell, "Weather-Related Power Outages and Electric System Resiliency," *Congressional Research Service,* Aug. 28, 2012, http://www.fas.org/sgp/crs/misc/R42696.pdf

## EXTREME WEATHER EVENTS

During the summer of 2012, a storm system referred to as a Derecho brought a series of thunderstorms, hurricane force winds, and a heat wave to the Ohio Valley and Mid-Atlantic states. The storm traveled 600 miles in only 10 hours, which left approximately 4.2 million customers without power throughout 11 states. Overall, the multi-day Derecho storm resulted in $2.9 billion dollars in damages and 28 deaths.[157]

Due to variances in the path and intensity of the storm, the highest reported electrical outages varied by state. "For example, West Virginia had 63 percent of electric utility customers without power after the storm, followed by Maryland with 33 percent, Virginia with 32 percent, and the District of Columbia with 25 percent."[158] These variances were dependent upon a number of factors including the recovery capabilities of utilities, additional storms resulting in a heat wave and/or fallen trees, and the intensity and range of damage to the components of the electrical grid in each state. Additionally, the recovery process after the Derecho storm took longer than other equivalent storms, such as Hurricane Ike or Irene, due to the lack of advanced warning given to utilities and state governments, as the storm developed over 18 hours from thunderstorms cells near the Chicago area into a wave of severe storms stretching from southern New Jersey to North Carolina.

Also occurring in 2012, Superstorm Sandy was a category three hurricane that caused extensive damage to the Eastern seaboard, specifically to New York and New Jersey, and resulted in 159 deaths. After the storm made landfall, 8.5 million customers were without power; one week later 1.3 million were still without power. Superstorm Sandy caused $65 billion in overall damages, with $14-26 billion in electrical outage costs[159], and approximately $8.3 billion in lost business in New Jersey.[160] The majority of the damage to electrical infrastructure was caused by storm surge.

Damage from floodwater can rust metals, destroy insulation, damage interruption capabilities, and impair trip units in molded-case circuit breakers. Additionally, components such as wire, cable, ground-fault circuit interrupters, lighting fixtures, surge protectors, motors, transformers, and other equipment must be replaced.[161] For

---

[157] "A Review of Power Outages and Restoration Following the June 2012 Derecho," *U.S. Department of Energy,* August, 2012, http://energy.gov/sites/prod/files/Derecho%202012_%20Review_0.pdfi thi

[158] Ibid.

[159] "An Ongoing Response to Hurricane Sandy," *The White House,* 2014, http://www.whitehouse.gov/issues/hurricane/sandy

[160] "Hurricane Sandy's Impact, By The Numbers (Infographic)," *Huffington Post,* Oct. 29, 2013, http://www.huffingtonpost.com/2013/10/29/hurricane-sandy-impact-infographic_n_4171243.html

[161] Jeff Griffin, "Disaster After the Disaster?" *Electrical Contractor,* May 2006, http://www.ecmag.com/section/safety/disaster-after-disaster

example, the ConEd substation along the East River exploded when a storm surge hit New York City. The damage to the substation caused 250,000 customers to lose power.[162] In an attempt to protect electrical equipment, PSE&G prematurely cut off service to approximately 500,000 customers due to flooding at multiple substations.[163]

The lessons of storms like the 2012 Derecho and Superstorm Sandy highlight the vulnerability of the grid to severe weather, the importance of weather prediction, the need for mutual assistance agreements, and the reinforcement of infrastructure. While the Derecho illustrated how buried electrical equipment is less vulnerable to severe storms, Sandy revealed the vulnerability of underground equipment to storm surges and flooding. These examples illustrate how preparations and solutions for severe weather will depend on the location of the infrastructure, risk analysis, and available resources.

## DROUGHTS, WILDFIRES, & EARTHQUAKES

In addition to Billion Dollar Storms, weather events such as droughts, wildfires, and earthquakes also threaten the security of the electrical grid. Low levels of water and high temperatures from droughts can affect multiple processes and components within thermo-electric plants, hydroelectric plants, gas-fired plants, photovoltaic cells, and transmission lines. For states such as California, which rely on multiple forms of energy generation, droughts can limit production from hydroelectric and nuclear power plants. In 2012, as temperatures hit record levels, it was estimated that hydroelectric plants in California would produce 1,137 fewer megawatts during the summer than in the winter. Not only is the electrical grid overtaxed, but utilities are forced to buy "replacement energy" to meet demands.[164]

Similar to droughts, wildfires can affect water availability, burn through transmission lines, and damage various components of grid infrastructure. Most dangerous to grid equipment are the particles contained in the smoke from the fires, which can ionize the

---

[162] Matt Sledge, Joy Resmovits, & Joe Van Brussel, "Hurricane Sandy Utility Outages May Be Worsened By Underinvestment, Lack of Planning," *Huffington Post,* November 2012, http://www.huffingtonpost.com/2012/11/01/hurricane-sandy-utility-outages_n_2053120.html

[163] Matt Sledge, Joy Resmovits, & Joe Van Brussel, "Hurricane Sandy Utility Outages May Be Worsened By Underinvestment, Lack of Planning," Huffington Post, November 2012, http://www.huffingtonpost.com/2012/11/01/hurricane-sandy-utility-outages_n_2053120.html

[164] Joe Eaton, "Record Heat, Drought Pose Problems for U.S. Electrical Power," *National Geographic,* August 2012, http://news.nationalgeographic.com/news/energy/2012/08/120817-record-heat-drought-pose-problems-for-electric-power-grid/

air and create electrical pathways away from the transmission lines. This process can shut down the lines, and possibly result in a cascading failure.[165]

Eight of the 12 costliest wildfires since 1980 occurred from 2002-2012; many of which threatened the electrical grid within California and other Western states.[166] In the summer-fall of 2012, the Western Wildfires burned 9.2 million acres of land throughout eight Western states. Additionally, in August of 2013 the Yosemite Wildfire (Rim Fire), endangered the Hetch Hetchy water and power system, which supplies water and electricity to the San Francisco area. The San Francisco Public Utilities Commission was forced to shut down two out of their three hydroelectric power stations due to the wildfire. As a result, SPUC was forced to purchase power on the open market to meet customer demand.[167]

For utilities located in California, the possibility of an earthquake damaging large sections of the electrical grid is a real threat. The 2011 Tōhoku Earthquake and the resulting meltdown at Fukushima nuclear power station illustrate the impact of a major tremor on vital infrastructure. Similar to other weather events, utilities must develop technology and implement best practices to mitigate the effects of earthquakes, which vary in magnitude and scope. In March of this year, a 6.9 magnitude earthquake hit off the coast of Northern California, only 50 miles from Eureka.[168] Not only do utilities have to harden the grid against the initial shockwaves, but from the resulting effects such as fires or aftershocks. Crews must also be trained to operate in those difficult environments.

## RESPONSE

Both the 2012 Derecho and Superstorm Sandy demonstrate the necessity for utilities and agencies on the state and federal level to coordinate preparation approaches before an extreme storm occurs. Especially during the Derecho, utilities were taken by surprise and underestimated the scope of outages and additional events, such as the subsequent heat wave, which made it extremely difficult for crews to repair the grid.

---

[165] "How Climate Change Puts out Electricity at Risk," *Union of Concerned Scientists,* April 2014, http://www.ucsusa.org/global_warming/science_and_impacts/impacts/effects-of-climate-change-risks-on-our-electricity-system.html

[166] "Billion-Dollar Weather/Climate Disasters," *NOAA: National Climatic Data Center,* 2013, http://www.ncdc.noaa.gov/billions/events

[167] Diana Marcum & Kurt Streeter, "Yosemite Fire one of the Largest in California History," *LA Times,* August 2013, http://www.latimes.com/local/lanow/la-me-ln-yosemite-fire-largest-california-rim-fire-20130824-story.html#axzz2wXGkKlpU

[168] Mark Stevenson, "Magnitude-6.9 Quake Strikes off Northern California," *NBC News,* March 10 2014, http://www.nbcnews.com/news/us-news/magnitude-6-9-quake-strikes-northern-california-n48676

The burden of preparation should be spread across multiple industries, including natural gas, water, and telecom due to the extensive damage to the infrastructure. For example, New Jersey Natural Gas, which serves approximately 500,000 customers, estimated that the damage from Superstorm Sandy cost $30-40 million dollars. Even a year after the storm, the utility is continuing to replace or re-pressurize 270 miles of damaged steel and cast iron main lines.

Additionally, many of these utilities rely on electricity to function. After the 2012 Derecho, more than 100 of the Washington Suburban Sanitary Commission facilities lost power, including the Potomac Water Filtration Plant that lost power for approximately 11 hours and implemented water restrictions that lasted for 36 hours after the storm. WSSC executives stated that all of their water and wastewater systems do rely on electricity to operate 109 facilities. All of the facilities, including 36 water storage facilities and two-water treatment plants, lost power during the Derecho storm. WSSC serves 460,000 customers within Montgomery and Prince George's Counties, yet the majority of the water treatment plans lack a backup power system.

After the Derecho, many telecom companies were unable to provide power to 77 emergency call centers, which serve more than 3.6 million customers throughout six states. According to data compiled by the FCC and telecom utilities, more than 2 million people in Virginia, Ohio, and West Virginia were unable to reach emergency services after 17 call centers completely lost service. Not only did many of these utilities lack back up power, but also many of the spare generators that were available did not function properly. Since the storm, the FCC has investigated the causes of the outages and ways to improve in preparation for a future storm. Ultimately, by mitigating risk throughout supply chains, electrical utilities can develop more progressive and effective responses and recovery practices.

Additionally, electrical utilities in California have begun to develop new technologies and methodologies to mitigate the effects earthquakes can have on grid infrastructure. The Pacific Earthquake Engineering Research Center has conducted studies with PG&E, which have focused on developing technology to implement at substations that receive and distribute electricity to large areas within California. Additionally, PG&E has focused on implementing methodologies to secure nuclear power plants from seismic activity. In 2012, the utility recently completed a 2D/3D onshore and a 3D offshore study of the ocean around the Diablo Canyon power plant; in 2013, the utility installed ocean-bottom seismometers.[169]

---

[169] "Seismic Safety at Diablo Canyon," *PG&E,* 2014, http://www.pge.com/safety/systemworks/dcpp/seismicsafety/

As these once atypical storms become more common, and increase in intensity, utilities have begun to develop mutual assistance agreements (MAA), which are voluntary partnerships between electric utilities throughout the country. In the wake of Superstorm Sandy, many utilities lacked the equipment or personnel to sufficiently restore power to customers in a timely manner. As a result, these MAA's provide predefined mechanisms to share industry resources expeditiously, while mitigating the risks and costs to member utilities that are associated with these weather events. [170]

In addition to MAA's, there are multiple other programs, which can provide utilities with spare equipment in the wake of an attack or an extreme weather event. The North American Reliability Corporation created the Spare Equipment Database (SED), a voluntary program for all Generator and Transmission Owners, where they can list if they have spare equipment.[171] In its inception, the database focused upon long-lead time transformers, such as generator step-up and transmission transformers, because this equipment is extremely expensive and can take more than six months to manufacture. Ultimately, this database was developed to complement existing MAA's and other equipment sharing programs, such as Edison Electric Institute's Spare Transformer Equipment Program (STEP).

To avoid future widespread outages, electrical, natural gas, and water utilities must work with each other and with the federal government to expand preparation capabilities, including bolstered information sharing techniques, stockpiles of spare equipment, and mutual assistance agreements.

## FEMA, NATIONAL GUARD & LOCAL AUTHORITIES

As the country's critical infrastructure continues to face these threats, Presidential Policy Directive (PPD) 8: National Preparedness was developed in March of 2011.[172] PPD 8 was formed to strengthen the security and resilience of the country by developing more effective emergency response plans, which could be implemented after a terrorist attack, natural disaster, or pandemic. As communities within the country continue to rebuild from Superstorm Sandy, federal agencies, local law enforcement,

---

[170] "Understanding the Electric Power Industry's Response and Restoration Process," *Edison Electric Institute,*

[171] "Special Report: Spare Equipment Database Storage," *NERC,* August 2011, http://www.nerc.com/comm/PC/Spare%20Equipment%20Database%20Task%20Force%20SEDTF%20DL/SEDTF_Report_Draft_PC_Meeting_2.pdf

[172] "Presidential Policy Directive/PPD-8: National Preparedness," *The Department of Homeland Security,* March 30, 2011, http://www.dhs.gov/presidential-policy-directive-8-national-preparedness

and first responders are developing new practices and implementing new policies to better respond to widespread disasters.

The Federal Emergency Management Agency (FEMA), in tandem with the Department of Homeland Security, developed multiple frameworks as part of the National Preparedness System requested within PPD 8. The various National Planning Frameworks are comprised of the National Prevention Framework, National Mitigation Framework, National Response Framework, and National Disaster Recovery Framework.[173] These documents are built upon three key themes: integration among the frameworks; engaged partnership with the whole community; and scalability, flexibility, and adaptability in implementation. It is imperative to integrate resources and processes into each of the frameworks, which can maximize the ability for agencies such as FEMA to sufficiently respond to an event.

In addition to the frameworks developed by FEMA, the agency has been an essential tool in recovering from natural disasters. After Superstorm Sandy in 2012, the federal government passed the Sandy Recovery Improvement Act (SRIA) of 2012, in which $50 billion was appropriated towards rebuilding and recovery processes facilitated by the Army Corps of Engineers and FEMA.[174] Through SRIA, multiple significant changes were made to how FEMA can deliver federal disaster aid to survivors, which included updates to debris removal procedures; a national strategy to reduce costs associated with future disasters; community disaster loans; and increased coordination between the Federal Transit Administration and FEMA regarding public transportation infrastructure. As of March of 2014, 14 out of the 17 proposed provisions were completed and implemented into pilot programs.[175]

In the wake of a major disaster such as Superstorm Sandy, FEMA has obtained assistance from the DOD's Defense Logistics Agency (DLA), the National Guard, and local authorities. In the hardest hit areas, such as New York and New Jersey, the DLA, National Guard, and police were tasked with delivering fuel to emergency vehicles, first responders, and residents. The DLA was responsible for filling "a 300,000 gallon FEMA order for points of distribution in Egg Harbor, West Orange, and Freehold, N.J.; and

---

[173] "Overview of the National Planning Frameworks," *The Department of Homeland Security,* May 2013, http://www.fema.gov/media-library-data/20130726-1914-25045-2057/final_overview_of_national_planning_frameworks_20130501.pdf

[174] Alex Rogers, "Superstorm Sandy, Six Months Later," Time, April 29, 2013, http://swampland.time.com/2013/04/29/superstorm-sandy-six-months-later/

[175] "Sandy Recovery Improvement Act of 2013," *Federal Emergency Management Agency,* March 4 , 2014, https://www.fema.gov/about-agency/sandy-recovery-improvement-act-2013

200,000 gallons to support three New York/New Jersey airfields."[176] Additionally, even as utility personnel were able to fix grid infrastructure, the DLA provided the New York/New Jersey area with hundreds of emergency generators.

In the weeks after the storm, more than 7,400 members of the National Guard from 11 states had responded to governors of 12 states and the mayor of D.C. as they declared a state of emergency. "Through mutual assistance agreements, Army National Guard ground and aviation task forces, from neighboring FEMA region states, are ready to meet gaps in mission command, communications, logistics, transportation, engineering, civil support, maintenance, security, and aviation."[177]

As physical attack or weather events continue to threaten the security of the electrical grid, utilities are beginning to develop new partnerships with the National Guard. In May of 2014, Florida Power & Light Company (FPL) announced that the utility has formed a partnership with the Florida National Guard. This partnership was designed to reinforce each organization's capabilities to natural and manmade disasters, specifically to hurricanes. With the logistics and operational experience of the Florida National Guard, FPL will be able to immediately leverage personnel and equipment in the wake of a disaster. This relationship will provide FPL with increased communications and the ability to sufficiently harden infrastructure before a storm hits, which will decrease the resulting damage. [178]

## SECURITY & INCIDENT RESPONSE

### ASSESSING GRID VULNERABILITIES

Not only is the U.S. electrical grid aging, but the structure of the components of the grid—transmission, distribution, and generation—also makes the grid inherently vulnerable to physical attacks. The majority of transmission and distribution lines, along with generator step-up high voltage (HV) transformers and substation step-down HV transformers, are located above ground and in remote locations. Vital to our electrical grid, these stations serve as the "on ramps and off ramps," respectively, of the national

---

[176] "DOD Provides Hurricane Sandy Response, Relief Update," *U.S. Department of Defense,* November 3, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118438

[177] Army Sgt. 1st Class Jim Greenhill, "National Guard Aids in Hurricane Sandy Response," *U.S. Department of Defense,* October 30, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118381

[178] "FPL and Florida National Guard form Historic, first-of-a-kind partnership to enhance disaster response capabilities," *May 2014,* http://newsroom.fpl.com/2014-05-02-FPL-and-Florida-National-Guard-form-historic-first-of-a-kind-partnership-to-enhance-disaster-response-capabilities

electrical grid transmission system. These components are vulnerable to a variety of physical attacks and are exposed to weather-related events such as hurricane force winds, flooding, lightning, or falling trees.

As mentioned throughout the roundtable sessions, it is necessary for federal agencies to formulate reliability standards to protect the grid from various types of attacks. The transmission components within the grid are regulated by both FERC and NERC, yet the distribution system is regulated on the state level. As a result, universal practices are not implemented, which has led to imbalances in security across the grid. According to statistics compiled by the Edison Electric Institute, approximately 90 percent of all power outages occur within the distribution system of the grid.[179] For utilities to sufficiently respond, mitigate, and recover from physical attacks, including weather-related events, it is necessary to focus on state-level regulations, as well as industry standards, for the distribution system of the grid.

At the behest of FERC, in the spring of 2014, NERC began to develop updated protection standards for critical transmission facilities and step-up and step-down substations. These standards, adopted at the May NERC board meeting and under preparation for FERC filing, specifically highlight the threat to the bulk-power system. Through this process, the existing bodies have highlighted a threat to the grid and issued instructions about addressing the threat. While there is an ongoing debate about the cost of these measures and their effectiveness, it is an example of how the FERC-NERC process assesses vulnerabilities and, resultantly, sets standards.

## INTELLIGENCE & FORECASTING

One of the most essential aspects of an efficient response to a physical attack or cyberattack is the preparation which comes before it. Through information sharing channels or sector-wide drills, electrical utilities are becoming better prepared to mitigate the effects of an attack.

Within the electrical sector, the Information Sharing Action Center (ES-ISAC) and the Electricity Sub-Sector Coordinating Council (ESCC), are two bodies in which utilities can share information concerning alerts, indicators, threat actors, and threat signatures. Not only can members of the industry coordinate policy to improve resilience and reliability, but this information is sent to the appropriate channels within the federal

[179] "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages," *Executive Office of the President,* August 2013, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf

government. The most important aspect of these information-sharing channels is the ability for the ES-ISAC and ESCC to facilitate the development of intra-sector relationships through the coordination of policies to increase grid reliability.

At the federal level, multiple agencies monitor the status of critical infrastructure including the National Cybersecurity and Communications Integration Center (NCCIC) at DHS. The NCCIC works with entities at the federal, state, and local levels, including law enforcement, to prepare, mitigate, and respond to cyber threats.[180] Through horizontal and vertical sharing, utilities will be able to develop an "integrated response plan" to an attack through more informed decision-making.[181]

Additionally, as more extreme weather events continue to threaten the security of the electrical grid, agencies are developing better tools to track storms to understand their impact upon critical infrastructure. IBM and NOAA developed a forecasting program called 'Deep Thunder' during the 1990's and have begun to implement this system. This model can assist utilities by providing a hyper-local analysis of the possible impact of a storm by examining historical examples. "Deep Thunder creates 24-48-hour forecasts at 1-2km resolution with a lead time of three hours to three days. Weather data can be coupled with analytics and visualization tailored to individual business needs."[182] This weather forecasting system has been used multiple times since its creation; notably during the 1996 Atlanta Olympic Games to examine rainfall patterns and will again be used during the 2016 Summer Olympic Games in Rio de Janeiro, Brazil to detect flooding and improve emergency response.[183]

## DRILLING & PREPARATION

As cyber and physical threats continue to advance, federal agencies such as DHS and NERC have held grid security exercises to assess the readiness and resilience of electrical utilities in the wake of an attack. In 2006, DHS sponsored the first government-lead full-scale cyber exercise in which over 115 different organizations, utilities, and levels of government participated. Since then, three more Cyber Storm exercises have occurred, with the most recent event in the fall of 2013. Not only did

---

[180] "Electric Power Industry Initiatives to Protect the Nation's Grid from Cyber Threats," Edison Electric Institute, Jan. 2013, www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf

[181] "Preparing Utilities to Respond to Cyberattacks," The Wall Street Journal: Deloitte Insights, Jan. 16, 2014, http://deloitte.wsj.com/riskandcompliance/2014/01/16/preparing-utilities-to-respond-to-cyberattacks/

[182] "Deep Thunder: Overview," IBM, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/deepthunder/

[183] "Deep Thunder: Transforming the World," IBM, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/deepthunder/transform/

Cyber Storm IV occur at the state and federal level, but countries such as Japan, Australia, and Sweden participated in the exercise.[184] In addition, NERC has held a series of two cybersecurity exercises, GridEx I and GridEx II, which occurred in the fall of 2011 and 2013. The GridEx drills were the first sector-wide grid security exercise and participants included utilities, organizations, and agencies from the U.S. and Canada. In the second GridEx drill, both cyber and physical attacks were simulated, which tested the ability for utilities to respond to multiple, yet interconnected threats.

These drills held by both DHS and NERC concentrated on similar goals and objectives, which included validating the current readiness of the electrical industry to accurately prepare, protect, and respond to a cyberattack; exercising various response plans of federal agencies and utilities in an attempt to evaluate areas for improvement; assessing current information sharing relationships, paths of communication, and the dissemination of information related to the attack without compromising national security; and practicing strategic decision making skills to sufficiently respond to incidents at the state and national levels. By conducting drills, such as Cyber Storm and GridEx, utilities, agencies, and governments can begin to implement successful practices to mitigate, respond, and recover from an attack.

Additionally, utilities have begun to conduct their own drills to measure their readiness and recovery processes. The Florida Power & Light Company (FPL) recently held a week-long storm drill, in which employees and members of the Florida National Guard had to respond to Category 3 "Hurricane Echo." The virtual storm made landfall in the Broward and Miami-Dade County area, before traveling north through the middle of Florida and exiting near Daytona Beach. Throughout the simulation, FPL employees assessed damage, tracked outages, communicated with customers and employees, and initiated service restoration. Overall, the Hurricane Echo simulation tested the utilities' storm plans and tactics, attempting to identify areas where progress can be made.[185]

---

[184] "Cyber Storm: Securing Cyber Space," *The Department of Homeland Security,* 2014, http://www.dhs.gov/cyber-storm-securing-cyber-space

[185] "FPL and Florida National Guard form historic, first-of-a-kind partnership to enhance disaster response capabilities," *Florida Power & Light Company,* May 2014, http://newsroom.fpl.com/2014-05-02-FPL-and-Florida-National-Guard-form-historic-first-of-a-kind-partnership-to-enhance-disaster-response-capabilities

## SPARE PARTS INVENTORY

As physical and cyberattacks continue to increase in severity, utilities have been forced to obtained spare parts to reinforce the integrity of the grid. Additionally, as events such as Superstorm Sandy or Metcalf demonstrate the threat to large swaths of grid infrastructure or one key facility, it is imperative that utilities have the ability to obtain spare parts to "keep the lights on" and their customers safe.

Currently, there are multiple voluntary partnerships in which electrical utilities can obtain critical components or personnel in the wake of a cyber or physical attack. MAAs have provided the sector with predefined mechanisms to share industry resources expeditiously, while mitigating the risks and costs to member utilities that are associated with damaging events. In addition, NERC created the Spare Equipment Database (SED), which is a program for all generation and transmission owners where they can list if they have spare equipment.[186] In its inception, the database was focused upon long-lead time transformers, such as generator step-up and transmission transformers because this equipment is extremely expensive and can take more than six months to manufacture. SED was formed to complement existing MAA's and other equipment sharing programs, such as Edison Electric Institute's Spare Transformer Equipment Program (STEP).

When building an inventory of spare components, utilities have been faced with the complexity of obtaining generation, transmission, and distribution assets. "There are a number of elements to a holistic spare parts inventory strategy for utilities, such as better part and component failure-rate data and analysis, better failure consequence analysis, improved workforce management, and of course predictive maintenance."[187] Considering that obtaining spare components is fairly difficult, utilities have begun to outfit grid infrastructure with sensors. This gives utility operators the ability to detect equipment issues before a widespread failure occurs through the process of predictive maintenance.

Utilities can monitor certain capabilities of infrastructure such as the temperature of transformers, the breakdown of insulation within cable connections, and transient analysis in various circuits. By outfitting grid infrastructure with sensors, utility personnel can make more targeted and precise repairs. Additionally, according to a survey

---

[186] "Special Report: Spare Equipment Databse System," *NERC,* August 2011, http://www.nerc.com/comm/PC/Spare%20Equipment%20Database%20Task%20Force%20SEDTF%20DL/SEDTF_Report_Draft_PC_Meeting_2.pdf

[187] Bill McBeath, "Smart Grid's Implications for Service Supply Chain," *ChainLink Research,* September 4, 2013, http://www.clresearch.com/research/detail.cfm?guid=648B1DE0-3048-79ED-99FA-A59C150FC6A4

conducted by DOE, applying a functional predicative maintenance program has the ability to reduce equipment breakdowns by 70-75 percent. Overall, equipment is replaced based upon its actual condition rather than on elapsed time since last maintenance or the hours of operational use.

## INCIDENT RESPONSE & INVESTIGATION

As physical and cyberattacks continue to increase in frequency and intensity, the 16 sectors of critical infrastructure have had to develop advanced response and recovery methodologies. In addition to the response practices developed by electrical utilities, agencies at the state and federal level most work in tandem to sufficiently respond after an attack.

As cyberattacks have become more advanced and affect electrical utilities on a daily basis, grid operators have integrated Software Management and Documentation Systems (SMDS) into SCADA systems. SMDS monitors all of activities of the control system, assisting IT and OT operators with an application restoration following a catastrophic event; control who may use any SCADA application system; and can control which actions can be performed. Additionally, Intrusion Detection Systems (IDS) can be implemented into control systems to recognize intrusions based upon unusual patterns of activity and communications attempted from an unauthorized address.

Recently U.S. and Israeli companies have been testing software developed by an Israeli security firm, which is designed to assist companies in reducing their incident response time in the wake of a cyberattack. "Large enterprises have a wide range of security products running on their endpoint systems or networks, including anti-malware programs, data-loss prevention (DLP) systems, firewalls and intrusion detection systems (IDS. These are further complemented by security information and event management (SIEM) products that analyze data from various applications and systems inside the organization and generate alerts."[188] The software, Hexadite Automated Incident Response Solution (AIRS), would reduce response time by using proprietary algorithms to instantly respond to security alerts and has the ability to investigate, contain, and remedy a security breach. AIRS was designed to complement existing systems by

[188] Lucian Cinstantin, "Israeli Security Startup Firm Hexadite Automates Cyber Incident Response," *Computerworld,* July 2, 2014, http://www.computerworld.com.au/article/549009/israeli_security_startup_firm_hexadite_automates_cyber_incident_response/

making them more efficient by ruling out false alarms and letting companies focus their resources on real threats.

Concerning physical attacks against grid infrastructure, incident response can be more complicated. Considering that co-ops, municipal, and investor owned utilities all have varying monetary, technological, and personnel resources at their disposal, incident response will differ. Additionally, authorities at the local level may not be equipped with the correct information or situation awareness to sufficiently respond to an event.

In April of 2013, multiple individuals attacked the PG&E Metcalf Substation, which has been described as "the most significant incident of domestic terrorism involving the grid that has ever occurred." [189] The individuals who attacked the substation strategically cut AT&T fiber-optic telecommunications cables, which hindered the ability of utility personnel to alert local authorities to the attack. Although, when local law enforcement personnel arrived at the scene, they concluded that nothing was suspicious and left. Since the attack, local FBI agents have been working with PG&E to understand the motivation and hopefully, find the perpetrators of the attack, yet no arrests have been made.

In response to the attack, PG&E intends to invest over $100 million over the next three years to improve security of various substations. These improvements range from upgraded cameras, better coordination with local law enforcement officers, improved lighting, and altering or removing trees and vegetation near substations. Additionally, Senator Jerry Hill, of San Mateo County, has introduced legislation, SB 699, which would require the Public Utilities Commission to develop security standards for utilities throughout California.[190]

As illustrated by Metcalf and experiences during severe storms, it is vital that utilities have the ability to communicate amongst themselves and with other sectors, even when telecommunications systems are disrupted. Dedicated radio spectrum for utility operators and channels for communications with state and local authorities can allow for better coordination of incident response and power recovery. The FCC should provide dedicated spectrum for utilities and develop procedures that reflect the importance of utility communications during or after an emergency.

---

[189] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *The Wall Street Journal,* February 5, 2014, http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778

[190] George Avalos, "PG&E will begin Metcalf Substation Security Upgrades this Year," *Contra Costa Times*, June 18, 2014, http://www.contracostatimes.com/news/ci_25988092/pg-e-expects-begin-metcalf-substation-security-upgrades

## INCIDENT RECOVERY

After a physical or cyberattack upon the electrical grid, the top priority for utilities is to ensure that the lights come back on in a safe and secure manner. Depending upon the scope and type of event, utilities may have to overcome multiple challenges to achieve their goal.

As demonstrated by the Metcalf attack in April of 2013, even though there was extensive damage to grid infrastructure, utility personnel were able to prevent a blackout by transferring power from the Silicon Valley area.[191] Considering that attacks against the grid at that magnitude are not common, electrical utilities must continue to participate in drills and develop response plans, which utilize personnel at the federal, state, and local levels. In addition, utilities must continue to develop positive intra-sector relations through MAAs and information-sharing bodies. By doing so, electrical utilities will be able to obtain critical components to grid infrastructure, such as transformers, in the wake of a physical attack.

The response to an event like Hurricane Sandy demonstrated how the MAAs were able to bring equipment from multiple utilities to the affected areas, and how the logistical support of military and National Guard assets provided needed transport and heavy lift capabilities.

Facing threats such as cyberattack or EMP, which would have potentially wide-reaching effects, incident response will require the ability to triage which systems require immediate power restoration for critical military, government, and civil facilities or services. Additionally, as demonstrated by the response of Saudi Aramco during the Shamoon attack, significant resources in terms of IT personnel and equipment may need to be deployed to rapidly isolate and replace infected or damaged computer equipment.

In replacing damaged transformer equipment, utilities can provide temporary equipment that can allow for quicker power restoration. It may be necessary to utilize the assistance of the military or National Guard to provide the heavy lift necessary to install and secure temporary replacement equipment for key facilities. Government and utilities can work together to store this equipment and plan for the prioritization and installation of this temporary equipment in the event of a major disruption.

---

[191] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *The Wall Street Journal,* February 5, 2014, http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778

An essential component of the recovery process for utilities after a physical or cyberattack is the black start procedure, which is the process of restarting transmission components after a partial or full shutdown. Power stations need an electrical supply to restart, which typically comes from the transmission or distribution system. Yet, in an emergency situation, the black start procedure involves turning on isolated power stations individually and, as they gradually begin to operate, they reconnect to each other and form an interconnected system once again.

Utilities have begun to integrate certain methodologies and technology to assist with their black starting capabilities. For example, the use of a microgrid can reinforce power generation, which, in turn, can quickly restart the transmission components within the grid. In addition, utilities also have small diesel generators, or Black Start Diesel Generators (BSDGs), which can be utilized to restart larger generators.

In the event of a major incident, it may be necessary to provide stockpiled or mobile BSDGs that can be moved to various generation sites for restoration. Following the 1989 Bay Area earthquake, Navy vessels used their turbines to provide black start capability. Additionally, in a microgrid environment, similar smaller-capacity generators could be used to power critical facilities such as military bases, government installations, and hospital facilities.

Finally, an important aspect of incident recovery is the ability for an electrical utility to share information and lessons learned from the event. Even lessons learned from minor incidents can provide insights into larger events. Some information may even presage a larger vulnerability or threat looming in the future. To this end, not only is intra-sector information sharing imperative through the ES-ISAC or ESCC, but also vertical sharing with federal, state, and local authorities to ensure that all proper channels have up-to-date and accurate information.

# EXECUTIVE BRANCH ACTION

It is encouraging for utilities that the Obama Administration has been actively engaged in the issue of grid security and cybersecurity, as it is clear the executive branch recognizes the importance of addressing the cyber vulnerabilities in critical infrastructure. In the current political environment, the president is capable of advancing cybersecurity and critical infrastructure policies without formalized legislation. Because of the current Congressional gridlock, this alternative pathway is necessary. While ideally both the executive and legislative branches will work together to improve grid security, in lieu of legislation, the Administration's actions are more critical than ever.

There is still more the executive branch can do to promote strong security preparation and practices. Further steps break down into three main themes: (1) facilitate and expand information sharing channels, especially between the public and private sectors; (2) delegate specific responsibilities to federal agencies; and (3) delegate responsibilities between federal agencies. Taken together, these three focuses will create a more efficient, streamlined federal government that is better equipped to handle system risks and threats.

Critical to this progress is the understanding that there are a number of federal agencies involved in security and cyber issues. Key federal actors include national security agencies like the Department of Homeland Security, Intelligence Community, FBI, law enforcement, and regulatory bodies like FERC and NERC. These organizations often have overlapping responsibilities, with a distinct lack of clarity about what each group's roles are or should be. Identifying relevant agencies, clarifying their roles, and eliminating wasteful overlap will have positive long-term effects for security practices.

Just as there are a variety of relevant agencies, so there are a variety of utilities with a stake in security policy. These utilities vary in size, geographic location, and role in the system. This means there can be no "one-size-fits-all" grid security policy, either in legislation or in executive action. Effective executive orders and presidential policy directives will take into account the variation in stakeholders, creating channels of horizontal information sharing (utility-to-utility) in addition to vertical information sharing (government-to-industry).

In the larger conversation on government action in utility security is industry frustration over the lack of comprehensive legislation. While this will be discussed further in the next section, these frustrations are relevant to the executive branch in that they give

the Administration the political ability and responsibility to take charge of the situation. That being said, working with the legislative branch to create common solutions with a larger foundation of support will still be more effective than executive action alone.

## RECENT ACTION

The Obama Administration has made two major steps forward in cybersecurity policy: Executive Order 13636 and its companion Presidential Policy Directive (PPD) 21, both released in February 2013. These actions then led to the creation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Concerns about antitrust violations in information sharing were subsequently addressed by the Department of Justice and the Federal Trade Commission. All these actions attempt to balance the proverbial "carrots and sticks" (rewards and punishments), although it is too soon to determine each initiative's efficacy.

### EXECUTIVE ORDER 13636

The most significant recent executive action is EO 13636, "Improving Critical Infrastructure Cybersecurity," released February 12, 2013. The order calls for increased and improved information sharing among relevant critical infrastructure sectors, both public and private; the development of a cybersecurity framework from NIST, completed by 2014; the establishment of a consultative process for continued review of cybersecurity and critical infrastructure threats; and privacy protection for relevant parties.[192]

In addition to its more theoretical statements, the EO also includes requirements that have specific deadlines. The only deadline still remaining is in February 2016, when regulatory agencies are required to report to the OMB on "any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements."[193] This report will then inform future executive or legislative policy that can remedy any issues. Such a requirement is an example of how the executive branch can create open lines of communication.

---

[192] U.S. President. Executive Order. "Improving Critical Infrastructure Cybersecurity, Executive Order 13636." *Federal Register* 78, no. 33. February 12, 2013: 11739. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. Retrieved June 26, 2014.
[193] U.S. President. Executive Order. "Improving Critical Infrastructure Cybersecurity, Executive Order 13636." *Federal Register* 78, no. 33. February 12, 2013: 11739. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. Retrieved June 26, 2014.

The EO also directs the Attorney General, Director of National Intelligence, and Secretary of Homeland Security to develop a process for declassification in order to share cyber threat information with the private sector. The location of the "tear line"—which separates classified from non-classified information—is extremely relevant to issues of information sharing from every perspective. While the military ultimately handles the day-to-day methods of and decisions about declassification, codifying the Administration's encouragement of moving the tear line is useful for utilities that need that support in their lobbying efforts.

This order also expanded Enhanced Cybersecurity Services, a DHS program which facilitates voluntary information sharing between government and critical infrastructure owners and operators. ECS collects and analyzes cybersecurity information from federal agencies and passes them on to Commercial Service Providers (CSPs), which then communicate that information to their critical infrastructure sector clients.[194] The executive branch can do more of this sort of supportive action, investing in and facilitating existing innovative solutions without relying entirely on new legislation.

At the same time, legislation remains a significant piece of the security puzzle. Roundtable participants agree that although EO 13636 was "a good start," comprehensive legislation is still necessary to address lingering concerns. Most of the goals and requirements of the EO are appropriately tangible and achievable, but they lack the force of legislation.

Critics of this executive order bring up several key points about the limits or dangers of relying on executive action. Testifying before the Subcommittee on Cybersecurity, Infrastructure, Protection, and Security Technologies during a July 2013 oversight hearing, cybersecurity expert Eric Fischer aptly summarized these critiques in five points:

1. "The order offers little more than do existing processes.
2. The order could make enactment of legislation less likely.
3. The process for developing the framework is either too slow or too rushed.
4. The framework risks becoming a form of de facto regulation, or alternatively, its voluntary nature makes it insufficiently enforceable.

[194] "Enhanced Cybersecurity Services." *Department of Homeland Security*. http://www.dhs.gov/enhanced-cybersecurity-services. Retrieved June 26, 2014.

5. The order could lead to over-classification or under-classification of high-risk critical infrastructure by DHS."[195]

Similar to Fischer's points, roundtable participants return to the carrot-stick analogy, reiterating that the executive order needs to expand its carrots to appease utilities.

While it is still too early for most analysts to determine the full success of EO 13636, some successes are clear. The NIST framework called for by the order (discussed in more detail further down) was completed and released in February 2014. Additionally, a May 2014 article from Reuters quotes the FBI as saying they had expedited security clearances with bank officials to warn them of potential cyber vulnerabilities. These expedited clearances were specifically called for in the EO.[196]

In relation to the grid in particular, the order may lead to excessive regulation of the electric sector. The EO does not differentiate between critical infrastructure sectors. Because the electric sector is one of the more experienced CI sectors when it comes to cybersecurity regulation, this one-size-fits-all approach can easily become a hindrance. While the electric sector clearly has not perfected its approach to regulation, it does have a better understanding of what might be necessary for cybersecurity than many other sectors. On the other hand, the electric sector's knowledge of regulation could be an advantage, as owners and operators of the grid could serve as leaders in implementing the EO.[197]

Like the other cyber-related sectors, the electric sector is also affected by the limited nature of the executive order. The EO has limited liability protection and limited funding, leaving private utilities concerned about the existing challenges and vulnerabilities this presents. It remains to be seen what the full effects of the EO are, but these shortcomings may continue to drive a wedge between the public and private sectors.

These limitations were conspicuously noted in a statement made by the Edison Electric Institute, an association representing all U.S. investor-owned electric utilities.[198] The EEI stated it shares the goals of EO 13636, agreeing that it is necessary to increase vertical and horizontal information sharing as well as establishing a cost-effective threat

---

[195] U.S. Congress. House of Representatives. Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Oversight of Executive Order 13636 and Development of the Cybersecurity Framework. 112th Cong., July 18, 2013.
[196] Joseph Menn. "FBI Says More Cooperation with Banks Key to Probe of Cyber Attacks." *Reuters.* May 13, 2013. http://www.reuters.com/article/2013/05/13/us-cyber-summit-fbi-banks-idUSBRE94C0XH20130513. Retrieved June 21, 2014.
[197] Stephen M. Spina and J. Daniel Skees. "Electric Utilities and the Cybersecurity Executive Order: Anticipating the Next Year." 2013. https://www.morganlewis.com/pubs/ElectricUtilities-CybersecurityExecutiveOrder_April2013.pdf. Retrieved June 16, 2014.
[198] "About EEI." *Edison Electric Institute.* http://www.eei.org/about/Pages/default.aspx. Retrieved June 26, 2014.

response. As many of our roundtable participants have said, though, the liability protection in the EO needs to be expanded and codified in legislation "to remove legal uncertainties and barriers to expanded cyber protection."[199]

Further effects of the EO remain to be seen, but its attempt to create new practices and codify the best existing practices is proof of the executive branch's critical support for grid protection.

## PRESIDENTIAL POLICY DIRECTIVE 21

PPD 21 on Critical Infrastructure Security and Resilience was released February 12, 2013, in conjunction with EO 13636. The purpose of the directive is to "advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." [200] Along the same lines, the PPD focuses on promoting integration and efficiency in approaching all cybersecurity issues.[201]

In terms of specific requirements and suggestions, the PPD 21 directs the executive branch to:

1. "Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time;
2. Understand the cascading consequences of infrastructure failures;
3. Evaluate and mature the public-private partnership;
4. Update the National Infrastructure Protection Plan;
5. Develop comprehensive research and development plan."[202]

While the overarching themes of PPD 21 mirror those of EO 13636, the two do differ in purpose. The best way to look at it is that the PPD and EO are two parts of the same goal: to strengthen critical infrastructure cybersecurity across sectors and public-private

---

[199] "Response to Executive Order 13636." *Edison Electric Institute*. April 29, 2013. http://www.ntia.doc.gov/files/ntia/eei_comments.pdf. Retrieved June 17, 2014.

[200] The White House. Presidential Policy Directive 21. "Critical Infrastructure Security and Resilience." February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Retrieved June 11, 2014.

[201] Fischer, Eric A. "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions." June 20, 2013. *Congressional Research Service*. http://www.fas.org/sgp/crs/natsec/R42114.pdf. Retrieved June 10, 2014.

[202] "Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive and (PPD)-21 Critical Infrastructure Security and Resilience." *Department of Homeland Security*. http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2012March13.pdf. Retrieved June 12, 2014.

boundaries. To accomplish this, the EO focuses primarily on political and legal goals, while the PPD outlines the logistical steps in implementing these requirements and suggestions.

Because of this, the PPD tends to be less glamorous and politically interesting, and it gets less news coverage than its EO cousin. Most sources discussing February 2013 executive action focus almost entirely on the EO, with some not even mentioning the PPD at all. This does not mitigate its importance, however, as PPD 21 shows the administration's commitment to the nuts and bolts of implementation in addition to headline-making rhetoric.

With this logistical intent in mind, the PPD outlines specific roles and tasks for all relevant federal departments and agencies, including DHS, the intelligence community, the General Services Administration, the Federal Communication Commission, and sector-specific agencies (DOE, in the case of the electrical grid).[203]

Regarding grid security, the PPD mirrors the EO and recent legislative action in addressing critical infrastructure more broadly, not just the electrical grid. This can prove a significant challenge to utilities and relevant agencies because the grid's strengths, weaknesses, and requirements are not the same as those of the other critical infrastructure sectors.

Utilities have responded publicly to these sorts of issues in relation to the EO (as discussed earlier in the EEI's comments), but they have not said anything substantial about PPD 21 specifically. Again, many experts and media outlets view the EO and PPD as two sides of the same coin, so responses to the EO often encompass responses to the PPD.

## NIST CYBERSECURITY FRAMEWORK

A direct result of EO 13636, NIST's Cybersecurity Framework was released February 12, 2014, nearly a year to the day after the EO that called for its creation.[204] The EO attempts to give weight and purpose to the framework, which sets up executive-

[203] U.S. Congress. House of Representatives. Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. *Oversight of Executive Order 13636 and Development of the Cybersecurity Framework*. 112th Cong., July 18, 2013.
[204] "NIST Releases Cybersecurity Framework Version 1.0." *National Institute of Standards and Technology*. February 12, 2014. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm. Retrieved June 12, 2014.

branch-sponsored performance goals and regulatory responsibilities.[205] This speaks to a larger attempt to make the framework more than "just another government report," as NIST gathered expert opinions from across sectors to make the framework as relevant and useful as possible.

The framework's goal is to connect relevant groups across sectors and promote best practices in cybersecurity. The structure of these best practices is meant to be risk-based, adaptable, and industry non-specific. While it will primarily benefit federal agencies, regulatory bodies, and utility operators, the framework is also meant to assist private industry and individuals. These groups can ideally use this framework to "create, guide, assess, or improve comprehensive cybersecurity programs."[206]

In response to repeated concerns about liability and privacy issues, the framework also aims to help organizations incorporate privacy and civil liberties into their cybersecurity measures.[207] To this end, it suggests methods of liability protection as well as asserting that information sharing does not inherently leave industry vulnerable to lawsuits. This is supported by the DOJ and FTC's April 2014 statement, discussed further down.

NIST refers to this framework as a "living document," one that can change its requirements and suggestions based on feedback from relevant sectors, changing technology and threats, and new regulations or legislation.[208] Although the impact of new legislation does not seem like it will be relevant any time soon given recent failures, it is still worth considering whether the framework would even be relevant if new legislation were passed. It is likely that any comprehensive cybersecurity legislation will look to the NIST framework for guidance. However, the flexibility of this framework still helps extend its usefulness in lieu of legislative action.

Some analysts and industry members are actively lobbying against NIST's framework. Two scholars worry that "the framework replaces the creative process of trial and error with a one-size-fits-all incentive: compliance with recommended federal standards."[209] This mirrors the too-many-sticks, not-enough-carrots complaint, as well as pointing out

---

[205] U.S. Congress. House of Representatives. Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. *Oversight of Executive Order 13636 and Development of the Cybersecurity Framework*. 112th Cong., July 18, 2013.
[206] "NIST Releases Cybersecurity Framework Version 1.0." *National Institute of Standards & Technology*. February 12, 2014. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm. Retrieved June 12, 2014.
[207] "Framework for Improving Critical Infrastructure Cybersecurity." *National Institute of Standards and Technology*. February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. Retrieved June 11, 2014.
[208] "NIST Releases Cybersecurity Framework Version 1.0." *National Institute of Standards & Technology*. February 12, 2014. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm. Retrieved June 12, 2014.
[209] Eli Dourado and Andrea Castillo. "Why the Cybersecurity Framework Will Make Us Less Secure." *Mercatus Center, George Mason University*. April 17, 2014. http://mercatus.org/sites/default/files/Dourado_CybersecurityFramework_v2.pdf. Retrieved June 12, 2014.

that the framework does not adequately take into account the varied nature of the industry. Utilities come in all different sizes and shapes (such as investor-owned vs. government-owned utilities), and their different needs mean they face different threats. By failing to offer a variety of incentives, the EO does not account for these different needs, and its recommendations as detailed in the NIST framework similarly gloss over key variations.

Like EO 13636, it is too early to tell what the full effects of the NIST framework will be. Early reports suggest that it is not as sweeping as the executive branch might have hoped, with its limits more notable than its capabilities. It is likely to be a starting point for further action to define key benchmarks and minimum standards for critical infrastructure cybersecurity. From the discussions at the project roundtables, it is clear that the framework is in no way a full substitute for legislative action.

## RELAXATION OF CONCERNS ABOUT ANTITRUST BEHAVIOR

On April 10, 2014, the Department of Justice and the Federal Trade Commission issued a statement saying that "they do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing."[210] This is significant in part because of the reputability of the two organizations involved, and also because it directly addresses one of the biggest concerns many industries have about information sharing.

The organizations' reasoning is related to the nature of cyber threat information, as it is "very technical" and also "very different from the sharing of competitively sensitive information." Cyber threat information sharing is not in the interest of profit or business achievement, but instead focused on the security of the American people.[211] This shows federal agencies' recognition of the importance of information sharing to the reduction of cyber threats, encouraging these vital information sharing public-private sector and private-private sector.

This joint action is clearly a step in the right direction, but it still does not go far enough. A verbal statement simply does not have the force that legislation or even an

---

[210] "Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information." *Federal Trade Commission*. April 10, 2014.
http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf. Retrieved June 12, 2014.
[211] "Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information." *Federal Trade Commission*. April 10, 2014.
http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf. Retrieved June 12, 2014.

executive order has, and that kind of definitive law is the only way to fully put liability concerns to bed. This is the common theme throughout all recent executive action: what is happening is positive, but it does not eliminate the need for comprehensive legislation.

## FURTHER STEPS

While recent executive action is a useful step forward for grid security, progress cannot end now. With or without legislation, the administration needs to either begin or continue to address information sharing, industry exchange, balance of agency responsibilities, and research & technology.

### ACTIONS ADDRESSING IMPROVED INFORMATION SHARING

Critical to all further grid security actions is improved processes of efficient information sharing. While the administration has made progress in this regard with EO 13636 and PPD 21, information sharing protocol still needs further clarification, codification, and encouragement from the executive branch. Any effective protocols will be timely, useful, and careful to include privacy and liability protection for private sector organizations.

To address cyber threats and attacks, information sharing processes must be understood from a variety of perspectives. It is not enough to clarify vertical sharing methods between federal governments and state and local governments. Effective information sharing processes must also include channels between the public and private sectors, horizontally from utility to utility, technologically from machine to machine (likely in an automated fashion), and on a micro level from individual to individual. Because there are so many parties who need available cyber threat information, limiting channels of communication to traditional top-down sharing might do more harm than good.

While the role of federal agencies can be over-emphasized, they are still critical to constructing a streamlined information sharing process. Roundtable participants emphasized that the EO does not sufficiently clarify the roles of DHS and NSA in communicating classified threat information. Too much regulation is a problem, as discussed earlier. Likewise, insufficient or confusing regulatory standards can leave the industry without much-needed guidance and leadership. This is especially relevant in

matters of national security, which are primarily the jurisdiction of the federal government, DHS, and the intelligence community. Day-to-day regulation of utilities is different from cyberattack incidents that threaten the entire United States Clarifying these differences in the roles of different regulatory bodies will strengthen security practices across the board.

Regarding national security issues, decisions about what classified information should be shared often err on the side of limited information sharing. Declassification of necessary information and/or increased security clearances for industry executives can help facilitate public-private information sharing. Not everything can or should be declassified, but moving the tear line can have significant effects both on threat preparedness and trust between sectors. This declassification is further discussed in a later section on legislation, which would codify such practices, but it is worth mentioning in any discussion of information sharing regulation.

While the bigger problem is lack of critical information sharing, excessive information sharing can also be problematic for industries. Roundtable participants have commented that information sharing without any kind of filter or screen can easily lead to information overload, bombarding utilities with information they do not need and therefore masking the information they do need. This may be part of workforce training, as the federal government may not actually understand what is important to utilities and what is not. Additionally, utilities may only know what is necessary day-to-day and not understand what information is pertinent for cyber threats. Establishing effective and accurate filters in information sharing will make acting on received information easier and more efficient.

## IMPROVED EXCHANGE TO-AND-FROM INDUSTRY

In order to establish the much-discussed public-private partnerships between government and industry, executive action can help facilitate improved exchange of people, data, and resources between utilities and government. This contributes to increased communication, a stronger understanding of the other sector's responsibilities, and improved trust between government and industry. Some of this exchange has occurred organically or through industry action, but it needs increased executive support to gain traction.

One of the first ways to achieve this exchange is by sharing labor. By developing workforce exchange programs, federal employees can temporarily work at utilities in the private sector, and utility employees can temporarily work in a relevant federal

department or regulatory body. This has significant benefits for workforce training, as an employee who is well-versed in both public and private sector grid security will be extremely useful to government or industry. The lack of understanding and trust between sectors may be one of the reasons collaboration has been inefficient. Addressing this issue through exchange programs improves this educational deficit.

While such exchange programs were not mentioned in EO 13636, the Department of Defense has expressed its support for the process. A July 2011 report emphasizes the DOD's commitment to creating such programs that facilitate and allow "'no-penalty' cross-flow of cyber professionals" between government and industry "to retain and grow innovative cyber talent."[212] The DOD is one of the most successful federal entities when it comes to establishing lines of communication and best practices between military, industry, and cyber experts.[213] Still it has faced its own challenges in implementing these programs. Other federal branches and agencies should follow the DOD's lead in spearheading innovative exchange programs—and where necessary, learn from the mistakes or shortfalls in DOD programs.

As discussed previously, exchange of data and information is critical to grid security. The exchange of raw data between public and private industries has in some instances been automated through new technologies. The first of these is Trusted Automated eXchange of Indicator Information (TAXII), an automated program started by DHS to "simplify and speed the secure exchange of cyber threat information."[214]

Another useful innovation is Cybersecurity Risk Information Sharing Program (CRISP). Like TAXII, CRISP is an automated data-sharing program gaining popularity in utilities. According to a report from the Bipartisan Policy Center, CRISP is a collaboration from private utilities, DOE, and national labs that "provides a near-real-time capability for critical infrastructure owners and operators to share and analyze cyber threat data and receive machine-to-machine mitigation measures."[215] CRISP is still in its pilot phase, but it is likely more utilities will adopt it over the coming years. Roundtable participants agree that technology like TAXII and CRISP are the future of cyber data exchange.

---

[212] "Department of Defense Strategy for Operating in Cyberspace." *Department of Defense.* July 2011. http://www.defense.gov/news/d20110714cyber.pdf. Retrieved June 12, 2014.
[213] Adam Stone. "DoD, private sector collaborate on cybersecurity best practices." *Federal Times.* May 7, 2014. http://www.federaltimes.com/article/20140507/CYBER/305070012/DoD-private-sector-collaborate-cybersecurity-best-practices. Retrieved June 12, 2014.
[214] "Frequently Asked Questions." *TAXII.* http://taxii.mitre.org/index.html. Retrieved June 12, 2014.
[215] "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat." *Bipartisan Policy Center.* February 2014. http://bipartisanpolicy.org/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf. Retrieved June 17, 2014.

Information Sharing and Analysis Centers (ISACs) also help facilitate this data exchange. There is a multitude of industry-specific ISACs, including a well-admired model in the financial sector. The Financial Sector Information Sharing and Analysis Center (FS-ISAC) began in 1999 to facilitate public-private information sharing regarding cyber threats. Its information and data sharing systems include law enforcement, government, intelligence organizations, and private industries, all from local to international levels.[216]

Because of its strong information sharing channels, the FS-ISAC has seen notable successes in recent years. A recent post on the White House blog commends the FS-ISAC for using its information sharing techniques to manage the "denial-of-service attacks" targeting top U.S. banks. Without the guidance and protocols of the FS-ISAC, banks would likely have been unprepared to handle such an attack.[217]

Another data exchange technique suggested by roundtable participants is the "LLC model." In this model, information would travel from utilities to a limited liability company (LLC) and then to the relevant ISAC. The inclusion of the LLC addresses concerns about liability, anti-trust violations, and information leaks. Participants note the LLC model has so far been used by a few electrical utilities, but there are plans to expand the program over the next couple years.

To coordinate this exchange of people and data, the federal government can set up institutions that assist the flow of resources between the public and private sectors. One such organization currently in existence is the Electricity Sub-Sector Coordinating Council (ESCC). Overseen by NERC, the ESCC aims to "foster and facilitate the coordination" of wide-reaching initiatives meant to "improve the reliability and resilience of the electricity sector" against physical and cyber threats.[218] These sorts of coordination councils can contribute to streamlining all current and future exchange programs. Executive initiatives establishing such councils also represent strong support from the executive branch for exchange of labor, data, and other critical resources.

---

[216] "About FS-ISAC." *Financial Services Information and Analysis Center.* https://www.fsisac.com/about. Retrieved June 17, 2014.
[217] Michael Daniel. "Getting Serious about Information Sharing for Cybersecurity." *White House Blog.* April 10, 2014. http://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity. Retrieved June 17, 2014.
[218] "Electricity Sub-Sector Coordinating Council Charter." *North American Electric Reliability Corporation.* May 12, 2010. http://www.nerc.com/comm/Other/Documents/Electricity%20Sub-Sector%20Coordinating%20Council%20ESCC/ESCC%20Charter.pdf. Retrieved June 17, 2014.

## BALANCING STREAMLINED & OVERLAPPING RESPONSIBILITIES

Among the many organizations and sectors involved in cyber and grid threats, there is overlap between and lack of clarity about what each group's roles are and should be. These roles need to be clarified and streamlined to increase efficiency. The existing organizations each have a role to play, but they cannot play those roles if there is too much overlap. At the same time, each group shares the responsibility to manage risk and respond to threats, so some overlap can actually increase threat preparedness and understanding. Critical to this discussion of overlap is the examination of the roles of DHS, ISACs, the FBI, and the entire intelligence community.

While the Department of Homeland Security addresses national security as a whole, its cybersecurity department is a leader in cyber research, understanding, and threat preparedness. This has also made it the lead agency in cyber protection of critical infrastructure, including the grid. In order to secure non-military cyber networks, DHS focuses on:

- "partnerships with owners and operators of critical infrastructure…;
- the release of actionable cyber alerts;
- investigations and arrests of cyber criminals; and
- education about how the public can stay safe online."[219]

This four-prong approach connects government, industry, and the broader public, promoting productive collaboration and communication for the sake of overall security.

Executive and legislative action has tried to clarify the role of DHS within the larger critical infrastructure and cybersecurity network, but there is still disagreement. Some see DHS as focusing purely on national security, but how should national security be defined as different from other critical infrastructure security issues? Proposed legislation tends to expand the powers of DHS, but that has also raised criticism about over-regulation of utilities. A clear understanding of what DHS's role is can clear up potentially dangerous confusion.

ISACs, discussed briefly earlier, also need a clearly defined role in information sharing and overall grid protection. The ES-ISAC, specific to the electricity sector, is meant to provide comprehensive grid analysis, which is then shared with the electric sector, other potentially relevant sectors, and government. ISACs also provide services such as risk mitigation, incident response and the sharing of information that is "accurate,

---

[219] "Cybersecurity Overview." *Department of Homeland Security*. http://www.dhs.gov/cybersecurity-overview. Retrieved June 12, 2014.

actionable, and relevant."[220] It is necessary both to improve ISACs information sharing methods and to distinguish them from other channels of communication and data exchange. If there is too much overlap in information sharing organizations, utilities will be swamped with too much information, unable to filter out and focus on what is actually important.

In the intelligence community, the FBI is one of the primary organizations working to establish cyber-focused public-private partnerships. The FBI's role in cybersecurity focuses on cybercrime, investigations, and penalties from a local to national level. One such inter-government FBI initiative is CyWatch, a cyber-monitoring organization connection the FBI to local and state governments.[221] The FBI also collaborates with other organizations in the intelligence community through groups such as the National Cyber Investigative Joint Task Force (NCIJTF), a cyber-response organization that includes intelligence community and law enforcement representatives. The NCIJTF came about as a result of Presidential Directive,[222] a strong example of the influence the executive branch can have in cross-sector coordination.

The intelligence community as a whole has a slightly different focus from the FBI, valuing information collection and sharing more than penalties. There are 17 member organizations in the community, including federal agencies, executive branch departments, and military organizations. Key organizations for grid security include the CIA, DHS, and ODNI (Office of the Director of National Intelligence).[223] The community's mission is to "collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties."[224] The focus of the community as a whole is information gathering, while individually each organization in the community has its own specific role.

Because it draws together so many relevant intelligence sectors, the intelligence community can be a useful model for integration and efficiency of grid-related sectors. There is some overlap among organizations, which can undermine the community's effective operation, but overall the idea that the group can have a broader focus than

---

[220] "Information Sharing and Analysis Centers (ISAC)." *National Council of ISACs*. http://isaccouncil.org/aboutus.html. Retrieved June 12, 2014.
[221] House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies. *The FBI's Role in Cyber Security*. 113th Cong., April 16, 2014. http://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security. Retrieved June 12, 2014.
[222] "Addressing Threats to the Nation's Cybersecurity." *Federal Bureau of Investigation*. http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1. Retrieved June 12, 2014.
[223] "Member Agencies." *Intelligence.Gov*. http://www.intelligence.gov/mission/member-agencies.html. Retrieved June 12, 2014.
[224] "Our Mission." *Intelligence.Gov*. http://www.intelligence.gov/mission/member-agencies.html. Retrieved June 12, 2014.

the individual unit is critical. Each member organization has the flexibility within the community to leverage its own strengths to contribute to a larger mission, while still retaining a unique purpose and sense of autonomy. The executive branch can encourage this kind of efficiency model in all its agencies, clarifying and codifying organizations' roles and the role of grid security groups as a whole.

## RESEARCH & TECHNOLOGY

Without advancements in grid security research and development, our critical infrastructure cannot keep up with continuously evolving physical and cyber threats. Ironically, as the grid becomes more technologically advanced and digitized, it becomes more vulnerable to cyber threats. These worthwhile improvements in grid efficiency must also be accompanied by an emphasis on grid security—especially as new technologies may result in new vulnerabilities. As a result, the federal government and private sector must continue to facilitate and support research in grid technology while stressing the importance of grid security improvements, product testing, security auditing, personnel training, and information sharing.

The Department of Energy has contributed to research through its collaboration in sponsoring CRISP, discussed earlier. The DOE should remain the sector-specific agency for electrical grid security, as they have the resources to bring together the products of national labs, private industry, and government. The DOE can take the lead on translating EO's and PPD's into the research and technology that would strengthen the grid.

The DOE's research arm is Advanced Research Projects Agency – Energy (ARPA-E). It was created in 2007 through a Congressional act emphasizing the need for energy research, and it began functioning in 2009. ARPA-E funds projects that advance energy sector research; in August 2013, ARPA-E was funding 285 projects related to energy, the environment, and national security.[225] Continued funding and support of this program will have direct benefits in the development of security technology and threat mitigation techniques.

The national labs are one of the primary ways government can and does support necessary research. The labs represent another mechanism of integrating government and private industry, as they are federally funded but operated by private sector

[225] "About." *ARPA-E*. http://arpa-e.energy.gov/?q=arpa-e-site-page/about. Retrieved June 12, 2014.

employees. Three national labs stand out in cybersecurity matters: Sandia, Idaho, and Pacific Northwest.

Sandia National Laboratories focuses on threat prevention and security by aiming to "develop protective technologies, conduct threat assessments, and analyze government, military, and civilian computer networks." One of their initiatives is the Cyber Engineering Research Institute (CERI) that works with academia and industry to research cybersecurity industries.[226] They have a far reach when it comes to integration of sectors, giving them more data and resources to work with.

Similarly, Idaho National Laboratory works with government, specifically departments like DHS, and private industry to develop solutions to national security issues.[227] In addition to overall security research, Pacific Northwest National Laboratory also provides funding for research focused specifically on cyber control systems to protect critical infrastructure.[228] The executive branch should support such research funding models, as they achieve the goals of increased information sharing, stronger communication channels, and better methods of building trust.

[226] "Cybersecurity." *Sandia National Laboratories.* 2014. http://www.sandia.gov/missions/defense_systems/cybersecurity.html. Retrieved June 12, 2014.
[227] "National Security." *Idaho National Laboratory.* http://www.inl.gov/nationalsecurity/capabilities/security/. Retrieved June 12, 2014.
[228] "Cyber Security: Protecting Our Nation's Critical Infrastructure." *Pacific Northwest National Laboratory.* June 2013. http://eioc.pnnl.gov/research/cybersecurity.stm. Retrieved June 12, 2014.

# LEGISLATIVE ACTION

Throughout the roundtable sessions, many of the participants voiced the necessity for comprehensive cybersecurity legislation to serve as a foundation for regulating and protecting various sectors—especially the electrical grid—against cyber threats. Even through there have been over 100 resolutions and bills related to cybersecurity introduced since the beginning of the 111th Congress, there has not been a major piece of cybersecurity legislation that has been signed into law since 2002. With the expansion of the capabilities of possible threat actors, this lack of legislation has left many aspects of critical infrastructure unregulated and vulnerable to attack.

Many of the obstacles that have hindered the ability for lawmakers to pass cybersecurity legislation include privacy and liability concerns related to information sharing within the post-Snowden environment; forming and implementing standards for critical infrastructure; the development of trust between the private sector and the federal government; and the designation of the roles and scope of federal agencies, such as DHS and NSA.

Additionally, one of the major challenges inhibiting the passage of new legislation is the varied nature of the industry. Electric utilities come in a variety of sizes, and they report to regulatory institutions both in the public and private sectors. There are also a multitude of government agencies, committees, regulatory bodies, and utility companies that have a stake in securing the grid. These organizations cross local, state, federal, and even international boundaries. As discussed previously, these organizations also have different—although sometimes overlapping—responsibilities. Legislation needs to be able to address these varied needs and avoid a one-size-fits-all mentality.

In addition the majority of the legislation that has been introduced within Congress has not focused specifically on the electrical grid but rather on the 16 sectors of critical infrastructure—the proposed GRID Acts and SHIELD Act are two exceptions, as they are specific proposals to the electrical grid. As our roundtable participants have said, the grid is the "most critical of critical" infrastructure, with its own unique set of legislative and regulatory demands. The U.S. electrical grid is facing more advanced threat actors with the capabilities to perpetrate cyber and physical attacks, which cause more damage at more frequent intervals. Critical infrastructure legislation must include provisions specifically formulated toward securing the electrical grid as it is an essential aspect of our country's national security.

## EXECUTIVE ORDER 13636 & THE NEED FOR LEGISLATION

In February of 2013, the Obama Administration released "Executive Order 13636: Improving Critical Infrastructure Cybersecurity," which reflected the electricity sector's need for a framework outlining a universal approach to implementing new practices and policies to deter cyberattacks. Based upon multiple roundtable discussions, there was a consensus among the participants that, although the Executive Order was a good start, legislation would be necessary to address various concerns. On a federal level, many institutions that are involved in securing critical infrastructure from cyberattacks must be reorganized to address private sector interests. For example, the Executive Order does not sufficiently address the roles of both DHS and the NSA in regulating the information sharing process. In this post-Snowden era, the private sector has become increasingly aware about securing sensitive material during the information sharing process with the government. To fully secure the electrical grid, it is imperative that utilities and federal agencies, including the Intelligence Community, have the ability to actively share information concerning cyber threats and threat actors.

Additionally, legislation is needed to establish the scope of cybersecurity regulations at both the state and federal level. There are many utilities that have expanded into multiple critical infrastructure sectors and have facilities within numerous states but need broader standards and benchmarks for key interstate issues.

## KEY TOPICS FOR LEGISLATION

- Information Sharing – Considered the most vital tool that legislation can provide in addressing both cyber and kinetic threats, there is agreement that channels between government and the private sector are necessary, as well as channels within the private sector, to improve risk assessment and situational awareness. While there are differing models for how this might be implemented—e.g. coordination centers, third-party operators, public-private partnerships—information sharing structures will ideally address methods of real time information sharing and protections for private, proprietary, or classified information. In addition, legislation must codify the role of multiple agencies within the federal government and the Intelligence Community within the information sharing process.

- Liability Protection & Antitrust Concerns – Even with the recent statement released by the FTC and DOJ, there are still questions concerning the ability to provide liability protection for the private sector to ensure that sharing information about a threat or vulnerability does not, in turn, leave a company vulnerable to legal or regulatory penalties. In addition to fostering information sharing between private sector entities, assurances are needed so that such information exchange is not viewed as collusion by antitrust regulators.

- Regulation & Incentives – A balance of the "sticks" of regulatory penalties with the "carrots" of financial or insurance incentives is necessary to build both support for and compliance with legislative proposals. Additionally, placing an emphasis on a "regulatory checklist" over an improved security culture will be counterproductive.

- Agency Responsibilities – There is growing consensus that the Department of Homeland Security, a civilian agency, will take the lead in critical infrastructure protection. It is important to consider these changes alongside existing roles for FERC, NERC, DOE, and the NRC.

- Cost Recovery – While generally handled by state utility commissions, with changing business models and increased security requirements there may be a need to discuss limited federal models for cost recovery.

- System Hardening, Supply Chain Protection, & Recovery Capacity – In many ways, the greatest deterrent to enemy attack is the ability to quickly respond and recover. Legislative solutions, combined with risk assessment and industry inputs, can provide resources, support, and security measures to harden key systems and ensure rapid recovery.

# A CATALOG OF SELECTED LEGISLATIVE PROPOSALS

## 111TH CONGRESS

*H.R. 5026: GRID Act (Grid Reliability and Infrastructure Defense Act)*

H.R. 5026 was sponsored by Representative Edward Markey (D-MA) and co-sponsored by Representative Fred Upton (R-MI). Markey introduced the GRID Act to the House of Representatives in April of 2010 and it was referred to the Energy & Commerce Committee. The GRID Act passed the House in June 2010, where it was referred to the Energy and Natural Resources Committee, ultimately dying in committee.[229]

This bill, unlike many others that have been introduced in Congress, was specific to the electrical grid. Overall, the bill amended the Federal Power Act and expanded the existing authority of the Federal Energy Regulatory Commission (FERC). With the expansion of FERC, the Commission would have been able to protect critical infrastructure from cyberattacks by issuing orders and regulations to the entire sector. H.R. 5026 would have given FERC more authority over the North American Electric Reliability Corporation (NERC), which currently has the legal means to form new regulations and reliability standards to mitigate cyber and physical attacks.

*S. 3480: Protecting Cyberspace as a National Asset Act of 2010*

S. 3480 was sponsored by Senator Joseph Lieberman (I-CT) and cosponsored by Senators Carper (D-DE) and Collins (R-ME). Lieberman introduced the bill in June of 2010 and it was referred to the House Homeland Security Committee, but it ultimately failed to progress within Congress.[230]

Overall, this bill aimed to expand the powers of the executive branch by amending the Homeland Security Act of 2002, which would have formed the National Center for Cybersecurity and Communications (NCCC) within DHS. The NCCC would work as a mediator between the private sector and various federal agencies by disseminating information, promoting technical advice, and identifying and evaluating the possible cyber risks to critical infrastructure. Most importantly, the President would have the authority to declare a national emergency period of 30 days if a cyberattack was perpetrated upon a piece of critical infrastructure.

---

[229] "H.R.5026 - GRID Act." *Congress.gov*. http://beta.congress.gov/bill/111th-congress/house-bill/5026?q=%7B%22search%22%3A%5B%22grid+act%22%5D%7D. Retrieved June 10, 2014.

[230] "S. 3480 – Protecting Cyberspace as a National Asset Act of 2010," *Thomas.loc.gov*, http://thomas.loc.gov/cgi-bin/query/D?c111:1:./temp/~c111qtA5GX::

## 112TH CONGRESS

*H.R. 3523: CISPA (Cyber Intelligence Sharing and Protection Act) – "CISPA 1.0"*

H.R. 3523 was sponsored by Representative Mike Rogers (R-MI) and cosponsored by 112 other Representatives. Representative Rogers introduced this bill to the House in November of 2011 and it was referred to the House Permanent Select Intelligence Committee; the bill passed the House in April of 2012. H.R. 3523 was then referred to the Senate Select Intelligence Committee, but it failed to pass within the Senate.[231]

This bill proposed to expand the National Security Act of 1947 to include new provisions concerning the topic of cyber threat intelligence and information sharing between federal agencies and the private sector. Related to information sharing, both the Director of National Intelligence (DNI) and the National Cybersecurity and Communications Integration Center (NCCIC), within DHS, would assist in obtaining and disseminating information related to cyber threats, actors, and attacks. Compared to other legislation, this bill did not address the development of standards for the regulation of critical infrastructure.

Minority Views: The Minority within the House Permanent Select Intelligence Committee voiced their concerns with H.R. 3523, citing the need for more provisions related to privacy and liability during the information sharing process. In addition, they were critical that H.R. 3523 did not provide specific restrictions concerning the volume or nature of the information that can be shared between the government and the private sector. Overall, the minority believed that the scope of the bill was too broad, noting the absence of clauses that would protect personal identifiable information (PII) from being disseminated during the information sharing process.

*H.R. 3674: PRECISE Act (Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2012*

H.R. 3674 was introduced by Representative Daniel Lundgren (R-CA-3) with 10 cosponsors, and was referred to the House Committee on Homeland Security, with additional referral to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Intelligence.[232]

Largely focused on the Department of Homeland Security, this legislation codified and strengthened the capabilities of DHS with regards to the protection of federal

[231] "H.R.3523 - Cyber Intelligence Sharing and Protection Act." Congress.gov. http://beta.congress.gov/bill/112th-congress/house-bill/3523?q={. Retrieved June 17, 2014.

[232] "H.R.3674 - PRECISE Act of 2012." Congress.gov. http://beta.congress.gov/bill/112th-congress/house-bill/3674?q=%7B%22search%22%3A%5B%22h.r.+3674%22%5D%7D. Retrieved June 10, 2014.

computer networks and the protection of critical infrastructure. Considered a response to the first iteration of CISPA, it mandated that DHS would serve as the lead agency for cybersecurity. It also created the National Information Sharing Organization (NISO), a non-profit private sector corporation tasked to manage information sharing within the private sector, standardize privacy protections, and coordinate information sharing between the private sector and government.

The PRECISE Act's definition of information sharing was more limited than that of CISPA 1.0, yet incorporated a more structured regulatory approach for critical infrastructure cybersecurity based on shared standards and risk assessments.

### *S. 2105: Cybersecurity Act of 2012*

The Cybersecurity Act of 2012 was introduced in the Senate on February 14, 2012. Sponsored by Senator Lieberman (I-CT), and co-sponsored by Senators Feinstein (D-CA), Rockefeller (D-WV), and Whitehouse (D-RI), the bill ultimately died in the Committee on Homeland Security and Governmental Affairs.[233]

S. 2105 proposed the expansion of the powers of the Department of Homeland Security, which would now include the ability for DHS to implement risk-based cybersecurity performance standards within critical infrastructure systems throughout the country.

Similar to the PRECISE Act's interest in creating NISO, the Cybersecurity Act called for the creation of the National Center for Cybersecurity and Communications (NCCC). This government entity would work with the private sector to secure and protect critical infrastructure, while also establishing stronger mechanisms for information sharing among sectors.[234]

### *S. 3414: CSA 2012*

S. 3414 was sponsored by Senator Lieberman (I-CT) and introduced to the Senate in July of 2012. This bill eventually died due to a failed vote for cloture in August of 2012.[235]

S. 3414 was a modified and expanded version of S. 2105, incorporating more regulation of critical infrastructure and protection of privacy concerns related to the information sharing process. CSA 2012 also called for the formation of a National

---

[233] "S.2105 - Cybersecurity Act of 2012." *Congress.gov*. http://beta.congress.gov/bill/112th-congress/senate-bill/2105?q=%7B%22search%22%3A%5B%22s.2105%22%5D%7D. Retrieved June 10, 2014.
[234] *Ibid*.
[235] "S.3414 - CSA2012." Congress.gov. http://beta.congress.gov/bill/112th-congress/senate-bill/3414?q=%7B%22search%22%3A%5B%22s.3414%22%5D%7D. Retrieved June 10, 2014.

Cybersecurity Council to be run by the Secretary of Homeland Security. DHS would also house a "Voluntary Cybersecurity Program for Critical Infrastructure" to educate critical infrastructure workers and enhance cybersecurity measures.[236]

CSA 2012 also allowed regulatory agencies to implement some cybersecurity practices as mandatory requirements. While a similar section appeared in the Cybersecurity Act of 2012, CSA 2012 expanded agencies' allowances. Like S. 2105, S. 3414 also expanded and codified the role of DHS, establishing it as the lead agency for domestic cybersecurity. DHS was charged with developing and implementing cybersecurity standards, as well as carrying out cyber-risk assessments.

## 113TH CONGRESS

*H.R. 624: CISPA 2.0 (Cyber Intelligence Sharing and Protection Act)*

H.R. 624 was sponsored by Representative Rogers (R-MI) and cosponsored by 37 other representatives. Representative Rogers introduced the bill in February of 2013 and it was referred to the House Permanent Select Committee on Intelligence. H.R. 624 passed the House in April of 2013 and is currently being debated within the Senate Select Committee on Intelligence.[237]

H.R. 624 is an expanded and modified version of the previous CISPA bill, H.R.3523. This updated version calls for real-time information sharing of threats between federal agencies, the National Cybersecurity Communications Integration Center (NCCIC) within DHS, and any other related organizations at both the state and federal levels. H.R. 624 continues to expand the role of the federal government by requiring DHS, the Attorney General, DOD, and the DNI to review cybersecurity policies and procedures related to privacy and liability concerns within the information sharing process. Most notably, this version of CISPA specifically states that PII will be protected.

Minority Views: Many in the minority support the alternations that were included within H.R. 624, but remain concerned that clauses pertaining to privacy and liability continue to be too broad. Consequently, the minority suggested that DHS serve as a point of contact for the private sector to quell any lingering fears concerning information sharing, privacy, and liability.

---

[236] *Ibid.*

[237] "H.R.624 - Cyber Intelligence Sharing and Protection Act." Congress.gov. http://beta.congress.gov/bill/113th-congress/house-bill/624?q=%7B%22search%22%3A%5B%22cispa%22%5D%7D. Retrieved June 10, 2014.

Roundtable participants noted that the primary difference between CISPA 1.0 and 2.0 is that the first bill states that information can be accessed and used to protect national security, but this clause is not included in CISPA 2.0. This speaks to the focus on increased privacy protection in CISPA 2.0 as a response to opposition of CISPA 1.0.

*H.R. 2417: SHIELD Act (Secure High-voltage Infrastructure for Electricity from Lethal Damage Act)*

H.R. 2417 was sponsored by Representative Trent Franks (R-AZ) and cosponsored by 24 other Representatives. Representative Franks introduced the bill in June of 2013 and it was referred to both the House Energy and Commerce and House Budget Committees.[238]

This bill referred to the 2008 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack which reported that natural (geomagnetic storms) and manmade EMP attacks pose a grave threat to the security of the U.S. electrical grid. H.R. 2417 would grant both the Federal Energy Regulatory Commission (FERC) and the President the ability to implement emergency measures in response to a threat or attack. Additionally, FERC would be responsible for overseeing the Electric Reliability Organization (North American Electric Reliability Corporation) in the formation of standards that would address hardening the grid against EMP threats through the application of best practices and new technology.

*H.R. 3696: NCCIP Act (National Cybersecurity and Critical Infrastructure Protection Act of 2013)*

H.R. 3696 was sponsored by Representative Michael McCaul (R-TX) and was cosponsored by Representatives Meehan (R-PA), Thompson (D-MS), and Clarke (D-NY). Representative McCaul introduced the bill in December of 2013 and it was referred to the House Committees on Science, Space and Technology and Oversight and Governmental Reform.[239]

H.R. 3696 would expand the Homeland Security Act of 2002 to include new provisions that would codify the role of the Department of Homeland Security as the federal agency responsible for this nation's cybersecurity mission. This bill aims to strengthen the National Cybersecurity and Communications Integration Center (NCCIC) as the

---

[238] "H.R.2417 - Secure High-voltage Infrastructure for Electricity from Lethal Damage Act." Congress.gov. http://beta.congress.gov/bill/113th-congress/house-bill/2417?q=%7B%22search%22%3A%5B%22h.r.+2417%22%5D%7D. Retrieved June 10, 2014.

[239] "H.R.3696 - National Cybersecurity and Critical Infrastructure Protection Act of 2013." Congress.gov. http://beta.congress.gov/bill/113th-congress/house-bill/3696?q=%7B%22search%22%3A%5B%22h.r.+3696%22%5D%7D. Retrieved June 10, 2014.

body regulating the information sharing process. H.R. 3696 fundamentally aims to strengthen the relationship between the federal government and the private sector, specifically through the establishment of a system designed to protect sensitive information (personally indefinable information) during the information sharing process.

### *S. 1353: Cybersecurity Act of 2013*

S. 1353 was sponsored by Senator John Rockefeller (D-WV) and cosponsored by Senator John Thune (R-SD). Senator Rockefeller introduced the bill in July of 2013 and it was referred to the Senate Committee on Commerce, Science, and Transportation.[240]

The bill, which is a revised version of the Cybersecurity Act of 2012, would expand NIST's authority in regulating critical infrastructure systems. It mirrors Executive Order 13636 (released February of the same year) in asking NIST to assemble guidelines that promote best practices in cybersecurity.[241] NIST came out with this Cybersecurity Framework in February 2014, so if this bill does get past committee, it is likely these portions of the bill will be revised.

Aside from NIST expansion, the Cybersecurity Act focuses on the development of cybersecurity research to improve threat preparedness and response. It also pushes for increased information sharing between the public and private sectors, a common theme in the majority of proposed cybersecurity legislation.

### *S.2158: GRID (Grid Reliability and Infrastructure Defense) Act 2.0*

The new GRID Act was introduced in the Senate in March 2014 by Senator Markey (D-MA), who sponsored the first GRID Act when he was in the House of Representatives. The bill is currently stalled in the Senate Energy and Natural Resources Committee.[242]

The bill is essentially the same as the version previously introduced by Senator Markey in 2010. Like the first GRID Act, this bill gives FERC the power to issue emergency orders and take on more regulatory responsibilities. Many utilities are still reluctant to support the bill, claiming it gives too much regulatory power to FERC.[243]

---

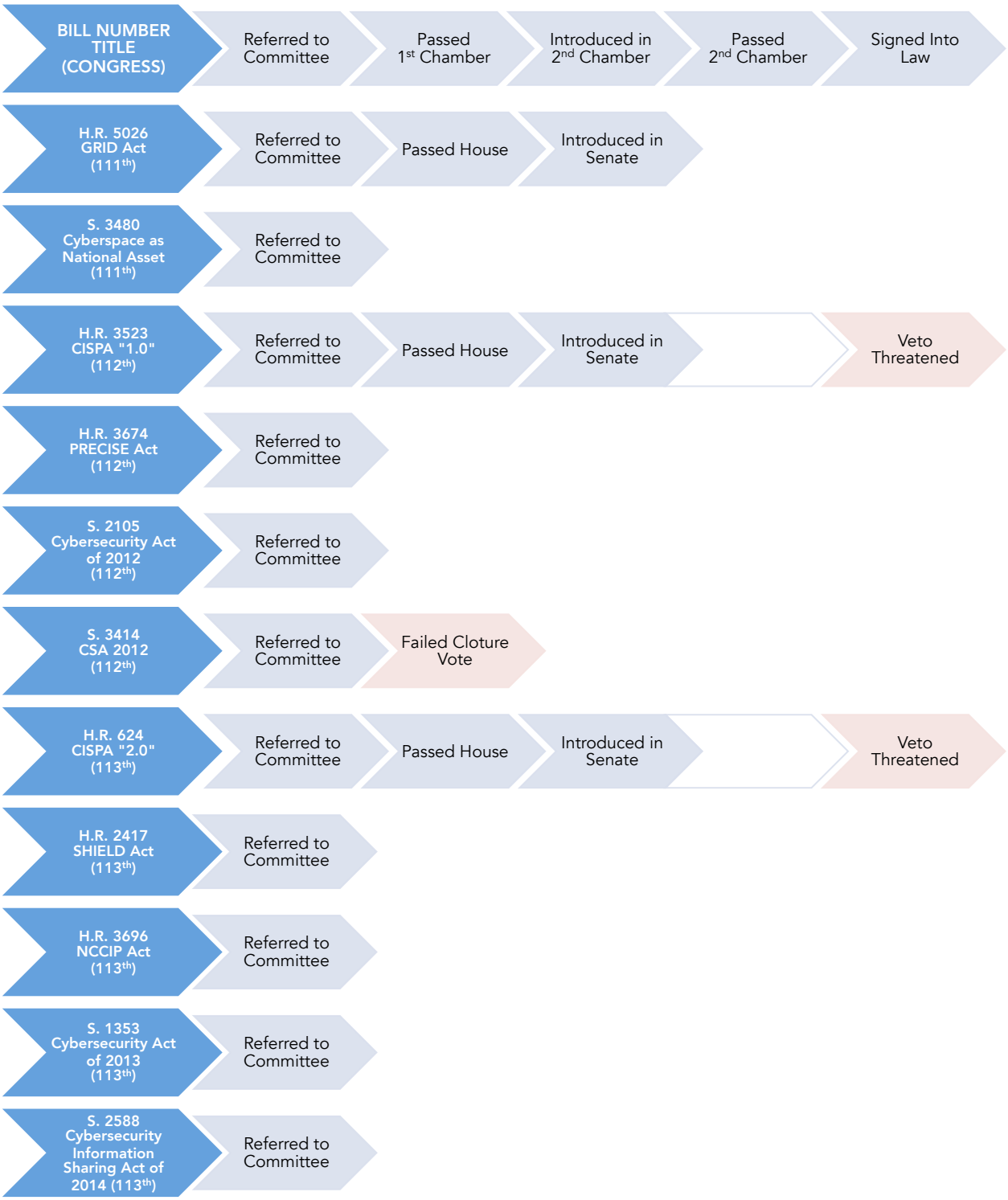
[240] "S.1353 - Cybersecurity Act of 2013." Congress.gov. http://beta.congress.gov/bill/113th-congress/senate-bill/1353?q=%7B%22search%22%3A%5B%22s.1353%22%5D%7D. Retrieved June 10, 2014.
[241] *Ibid.*
[242] "S.2158 - GRID Act." *Congress.gov.* http://beta.congress.gov/bill/113th-congress/senate-bill/2158?q=%7B%22search%22%3A%5B%22s.2158%22%5D%7D. Retrieved June 10, 2014.
[243] Timothy Cama. "Bill would give feds new power to protect electric grid." *The Hill.* March 26, 2014. http://thehill.com/policy/energy-environment/201834-bill-would-give-feds-new-power-to-protect-electric-grid. Retrieved June 24, 2014.

*S.2588: CISA: Cybersecurity Information Sharing Act*

The Cybersecurity Information Sharing Act is the most recent attempt to pass cybersecurity legislation through Congress and is fundamentally similar to H.R. 624 (CISPA), which passed the House in April of 2013. Last week. CISA advanced in a 12-3 vote out of the Senate Intelligence Committee, yet is facing opposition within Congress and from privacy groups. The aim of CISA is to increase information sharing; strengthen liability protection; establish a DHS 'portal' for depositing information that will then be disseminated to the appropriate federal agencies; and would limit government's ability to inappropriately use cyber information for regulation or investigation.

Before the bill passed the Intelligence Committee, amendments were added which further strengthened privacy protection and would require the federal government to adhere to protocols that protect individuals and limit federal power. Although, many privacy groups believes that CISA would facilitate the flow of private information and communications data to agencies, specifically NSA. Legislators who voted for the bill believe that CISA or CISPA is the first step towards increasing cybersecurity and deterring the ability for threat actors to attack critical nodes of U.S. society.

# PROGRESS OF SELECTED LEGISLATION



## CODIFYING NIST STANDARDS

In the absence of cybersecurity legislation, actors within the public and private sectors have taken multiple steps to secure the grid and increase reliability. However, without codified standards to which electrical utilities on a national basis must adhere, sections of the grid are not being updated to mitigate, deter, and recover from 21st century threats. As a result, the Obama Administration, through EO 13636, tasked the National Institute of Standards and Technology to develop a voluntary, risk-based cybersecurity framework. As a government agency, NIST has the weight of executive support and power behind it; yet, the agency focuses on technology and research, which naturally creates a relationship between the agency and private research institutions and industry.[244]

The Framework for Improving Critical Infrastructure Cybersecurity, which was released in February of 2014, provides entities in the 16 sectors of critical infrastructure with a structure that customers, regulators, and organizations can implement to increase security. By applying this document to their current operating procedures, organizations can assess their level of security against cyber threats. By doing so, practical plans can be formulated and practices can be implemented, which deter and mitigate cyber threats. Most importantly, this framework has been described as a "living document," meaning that NIST intends to update the information as new threats or attacks occur.[245]

Overall, the role of NIST is essential as it acts as a bridge between the federal government and the private sector. In February of 2012, NIST released the Smart Grid Framework, which laid the foundation for utilities' implementation of new technology. Similar to the recently released Cybersecurity Framework, the Smart Grid Framework promotes best practices and provides a model for information sharing and public-private partnerships.[246] Ultimately, in the absence of legislation, NIST has provided a way to promote universal standards without demanding compliance.

---

[244] "What we do." *National Institute of Standards and Technology*. http://www.nist.gov. Retrieved June 12, 2014.
[245] "NIST Releases Cybersecurity Framework Version 1.0," *NIST.gov*, Feb. 12, 2014, http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm
[246] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0." *National Institute of Standards and Technology*. February 2012. http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf. Retrieved June 10, 2014.

# FURTHER STEPS

Roundtable participants and analysts agree that comprehensive legislation is necessary to secure the electrical grid against cyber and physical attacks. This legislation must include a few key topics in order to be effective: filling agency positions, liability issues, information sharing, incentives, and workforce education.

## FILLING KEY ROLES IN EXECUTIVE AGENCIES

Empty positions in federal agencies are an unavoidable drawback of government turnover. Efficient government, however, depends on regularly filling these roles promptly. Timeliness in the whole process, including nominations and confirmations of agency heads, will increase the stability of government agencies. As we approach the presidential transition in 2016-17, it is vital that the new president is able to quickly fill key posts, while still respecting the prerogatives of the Senate.

Filling empty positions also strengthens the overall government hierarchy, clarifying which people and organizations are in charge during a threat situation. This stability is especially important in cyber-related industries, where a lack of threat preparation and crisis management can have catastrophic effects.

## ADDRESSING ISSUES SURROUNDING LIABILITY

According to roundtable discussions, one of the primary concerns many utility companies and private industries have regarding grid/cybersecurity legislation is the perceived lack of liability protection. The private sector needs to have the ability to share information about risks and threats without subsequently leaving themselves vulnerable.

In order to facilitate trust between the public and private sectors, there needs to be information sharing between the two sectors that is unclouded by the threat of liability. There is no way to establish that trust if industries believe they will be punished for their honesty.

With this dynamic in mind, comprehensive legislation can help clarify and codify liability protections in information sharing. Several bills have failed in part because of the limits of their protection clauses. An extension of this liability protection might then help a bill move forward in the legislative process.

As mentioned in the previous section, a recent joint statement from the Department of Justice and the Federal Trade Commission notes that concerns about antitrust issues are not an obstacle to sharing information regarding cyber threat information. The DOJ and FTC clearly state that industry will not be liable for collusion or antitrust violations for sharing relevant cyber threat information. This opens the door for legislation that gives industry more leeway in information sharing.

## COORDINATING INFORMATION SHARING

Preparing for and handling cyber or physical attacks to the grid requires information to get to utilities in a timely, usable manner. Too much information all at once, or too little too late, can have catastrophic effects on the system. Information sharing must also be coordinated vertically and horizontally, creating channels that can cross federal-state boundaries and public-private divisions.

The first part of this information sharing process is timeliness. Roundtable participants noted that ideal information sharing structures would have "real-time" information sharing, so that as any part of the grid-related sectors receives relevant information, they would be able to transmit that information to the appropriate places. This also refers to the automated information sharing present in new Smart Grid data, as electrical operators can collect this monitoring and analysis data in real time.

Timeliness must exist alongside usability. If there is too much information shared then there is no way to quickly and accurately sort out pertinent information. Setting up effective filters on information sharing, perhaps through automated measures, could reduce the excess of unusable information that comes from many of these new technological advancements.

Crucial to this sort of sensitive information sharing is the location of the "tear line" in classified documents. A reference to traditional military documents, the tear line is defined as "a physical line on an intelligence message or document which separates categories of information that have been approved for foreign disclosure and release."[247] Any information below the tear line is cleared for disclosure, whereas intelligence above the tear line is kept classified. If the tear line is too high, there is potential for an excess of sensitive intelligence being released to the private sector unnecessarily. Conversely, if the tear line is too low, information that could be essential

[247] Department of Defense, "Tear Line." *About.com*. http://usmilitary.about.com/od/glossarytermst/g/t6294.htm. Retrieved June 23, 2014.

to utilities preparation might be withheld and have significant negative results. Finding the appropriate tear line could be the difference in preventing a catastrophe. Since this is such an important aspect of information sharing, determining where the tear line is must be considered diligently.

Of course, not all cyber-related information can or should be declassified, but the fact remains that relevant private or governmental industries all need to be kept in the loop in order to do their jobs efficiently and effectively. Furthermore, it is important to standardize this tear line location as much as possible to avoid excessive subjectivity or conflicts of interest between parties. Declassification of information is time-consuming and difficult, but in the long run it is necessary for effective communication among sectors.

The relationship between sectors is also critical to the logistics of information sharing. Because the electrical grid is relevant across state lines and across sectors, there needs to be standardized information sharing regulations across the board. It is necessary to have communication channels between federal and state governments, between government and private industry, and between different industries. This communication network will allow for the flow of information to all relevant parties.

Some utilities have unique perspectives on the information sharing process. For example, investor-owned utilities (IOUs) have a board of trustees that has a particular stake in the security of the industry.

Because of this perspective, IOUs participated in high numbers in 2013's GridEx II security exercise (discussed previously). The Executive Tabletop discussion at the end of the exercise also included several CEOs and investors from private industry.[248] Any discussion of grid security must take into account that there are a variety of stakeholders in this issue. IOUs' particular stake may make them more reluctant to advocate information sharing without strong PII protection.

Regarding legislation, any bill that facilitates information sharing will have a number of perspectives and stakeholders to incorporate. The legislative branch must use this as an opportunity to work with the executive branch to create legislation and executive orders that are complementary. If it is not feasible for one bill to include the many facets of information sharing (stakeholders, declassification, state boundaries, etc.), an

[248] "Grid Security Exercise (GridEx II): After-Action Report." *North American Electric Reliability Corporation*. March 2014. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf. Retrieved June 17, 2014.

effective executive order or presidential policy directive might be able to fill some, but not all gaps.

## ADDRESSING FINANCIAL & INSURANCE INCENTIVES

The incentive structure in the electrical grid is off-balance, according to experts and roundtable participants. Following the "carrot-stick" analogy (carrots as rewards and sticks as punishments), the current system has too many sticks and not enough carrots. Legislation should help facilitate a new balance, one that does not over-emphasize regulation at the cost of trust and goodwill among sectors.

Government must find new incentives, both financial and insurance-based, for utilities to follow rules and regulations without depending entirely on mandatory compliance. Incentivizing regulations increases support for them, which not only helps legislation get passed, but also ensures its ultimate effectiveness. Government can achieve this revised incentive structure in at least three ways: providing research grants, building public-private partnerships, and continuing communication with industry to identify their needs and wants.

Offering research grants to national labs, universities, and other research-oriented organizations is one of these potential carrots. These government grants would incentivize much-needed research and development, encouraging labs to focus on advancing our understanding of cyber and physical threats to critical infrastructure. Providing funding instead of mandates changes the dynamic between researchers and government, fostering an environment of progress.

In a broader sense, the relationship between government and the entire private sector is critical to grid security. Building effective public-private partnerships (PPPs) between federal and state governments and the utility industry leads to increased collaboration and stronger solutions to cyber threats. These PPPs can focus on several weak areas of the system. Roundtable participants specifically pointed to replacing transformer reserves, warehousing equipment, and logistical support. Combining private sector resources, government capabilities, and the technical advancements of national labs and tech companies leads to effective electrical grid security.

None of these advancements would be possible without an established line of communication between government and industry. Legislators and federal agencies cannot provide useful incentives to industry without having a clear understanding of

what industry wants. This sort of relationship will open the door for other relationships along the way.

## EDUCATING THE WORKFORCE

Advancements in grid security are not possible without workers who are experienced in and /or educated about cybersecurity threats. To this end, several education programs have been launched recently for both current and potential cyber workers.

One such workforce education program is the National Initiative for Cybersecurity Education (NICE), led by NIST. The NICE cybersecurity education program is meant to be "sustainable and continually improving," teaching workers to use "sound cyber practices" that will contribute to national security efforts.[249] NICE has also developed a National Cybersecurity Workforce Framework with the intention of defining the cyber workforce and codifying its best practices.[250]

The Department of Homeland Security also supports a variety of cyber education initiatives, including the National Initiative for Cybersecurity Careers and Studies (NICCS), CyberSkills Management Support Initiative (CMSI), and the IT Security Essential Body of Knowledge (EBK).[251]

This education is especially critical given the current culture. The workforce is aging, and young people need to be prepared to take their place. Grid security does not depend only on technological advancement, but on a skilled, capable workforce that can effectively utilize available data and technology. This skill should not be limited to post-high-school development, but should be incorporated in STEM (Science, Technology, Engineering, and Math) education for younger children. Increasing STEM education with a strong cyber component will prepare students for a variety of careers and give them opportunities they may not have had otherwise.

At the same time, education must be available not just for students considering cyber-related careers, but also for those currently in the cyber workforce. Cyber-related fields are especially dynamic because the technology keeps changing. Workers who were trained 20 years ago may actually know less about the current industry than newly-

---

[249] "About." *National Initiative for Cybersecurity Education*. http://csrc.nist.gov/nice/. Retrieved June 12, 2014.
[250] "Highlights." *National Initiative for Cybersecurity Education.* http://csrc.nist.gov/nice/index.htm. Retrieved June 24, 2014.
[251] "The Cyber Workforce; the Next Generation of Cyber Leaders." *Department of Homeland Security*. http://www.dhs.gov/cyber-workforce-next-generation-cyber-leaders. Retrieved June 12, 2014.

educated workers. Offering technical classes—some voluntary, some mandatory—to these workers will help improve the workforce as a whole.

Expanding programs like this through additional funding and support has long-term benefits for grid security, cybersecurity, and overall national security. It does not matter how advanced grid technology is if workers do not know how to operate and utilize it. In order to promote an efficient, secure electrical grid system, the workforce needs educational opportunities and support.

## "LEGISLATING TRUST"

Ultimately, you cannot legislate trust. While legislation can create channels of communication, or facilitate a carrots-over-sticks regulation method, trust cannot be proscribed or mandated. In a post-Snowden era, trust is even more difficult to establish. Concerns about liability, privacy, and classified information create barriers between the public and private sectors.

Establishing trust may be difficult, but it is critical to every part of this conversation. Roundtable participants mentioned multiple times that the electric sector does not want to be regulated, so mandatory regulations lead to reluctant—and likely less efficient—compliance. Innovation and efficacy do not come from environments of mistrust.

# FEDERAL, STATE & LOCAL INTERACTION

## UNIQUE ROLE OF STATES

State and local government will play a significant role in grid security solutions and the response to any incident. With power distribution regulated at the state level, state utility commissions and independent system operators will shape regulatory incentives and cost recovery models for improved security measures. State and local involvement is integral to the effective implementation of new technology, the diligent preparation for unforeseeable events, and the immediate response to those events.

States play a unique role in this process, and the effectiveness of state and local involvement cannot be overlooked. Public utilities commissions are a particularly valuable tool. A public utilities commission is a regulatory body within a state that is in charge of the operations and maintenance of utility companies in that state.[252] A continual theme throughout this report will be the relationship between the public and private sector, and the role of the public utilities commission is essentially to bridge the gap between government regulations, industry standards, and public demand.[253] The public utilities commissions would need to play a significant role in the implementation and maintenance of such technology, as it is essential to the cooperation between federal and local authorities.

Another asset of state involvement is the use of independent system operators. FERC states that independent system operators are a method to provide non-discriminatory access to transmission.[254] These independent system operators work within a finite geographical area, typically limited to one state. This allows for optimal familiarization with the needs of the specific area, a key reason why their cooperation with the federal government is essential for the success of the project. These independent system operators ultimately led to the formation of Regional Transmission Organizations (RTO), which increase transmission access and efficient operations on a regional level. The primary benefits of these RTOs are their effectiveness at creating interstate grid

---

[252] "About NARUC." *National Association of Regulatory Utility Commissioners.* http://www.naruc.org/about.cfm. Retrieved June 20, 2014.

[253] "Mission Statement." *North Carolina Utilities Commission.* http://www.ncuc.net/. Retrieved June 20, 2014.

[254] "Regional Transmission Organizations (RTO)/Independent System Operators (ISO)." *Federal Energy Regulatory Commission.* http://www.ferc.gov/industries/electric/indus-act/rto.asp. Retrieved June 20, 2014.

interaction and their coverage of a larger geographic area. [255] While these bridges between the federal government and local authorities are extremely helpful in both the preparation and responses to an incident, the issue of cost recovery is still a large concern.

Often the cost burden falls disproportionately on the state government. This is due to a number of reasons, but a main reason is that the state government typically assists utilities in funding innovative grid projects. For example, New York governor Andrew Cuomo allotted $40 million in prize money to develop microgrid technology after Superstorm Sandy.[256] If there is an incident that destroys all of these developments, there is no federal government insurance policy that will reimburse the state of New York—the $40 million is a sunk cost. This, in addition to the ongoing investments made by state governments regarding electrical grid innovation, adds up to be a hefty sum on the state government. Once again, this ties together both the state and federal governments, as well as private investors.

Dividing up these costs of innovation can alleviate the burden on the state government, allowing the state governments to be better financially prepared for an incident. One primary problem with dividing up these costs lies with politics. Pouring money into innovative grid technology is not popular amongst voters, so lawmakers typically send funds elsewhere. This is particularly true at the federal level, as spending federal money towards innovation in a specific state is even more unpopular nationally.

Although unpopular, measures have been taken by the federal government to expedite the technological development of the grid; and both Smart Grid and microgrid technology has been invested in at both the state and federal level. The Smart Grid Investment Grant program is managed by the Department of Energy, and was authorized by the Energy Independence and Security Act of 2007. Funded by the American Recovery and Reinvestment Act of 2009, the efforts seek to further develop and implement Smart Grid technology using the $3.4 billion grant.

As of a 2012 progress report, spending and implementation are on track based on original projections. [257] This proactive effort by the federal government is promising, and it has boosted statewide efforts to develop the technology as well. In Connecticut,

---

[255] "Regional Transmission Organizations (RTO)/Independent System Operators (ISO)." *Federal Energy Regulatory Commission*. http://www.ferc.gov/industries/electric/indus-act/rto.asp. Retrieved June 20, 2014.

[256] http://www.greentechmedia.com/articles/read/new-york-plans-40m-in-prizes-for-storm-resilient-microgrids

[257] "Smart Grid Investment Grant Program: Progress Report." *U.S. Department of Energy*. July 2012. http://energy.gov/sites/prod/files/Smart%20Grid%20Investment%20Grant%20Program%20-%20Progress%20Report%20July%202012.pdf. Retrieved June 19, 2014.

the Department of Energy and Environmental Protection has established a Microgrid Pilot Program. The state has invested $18 million to develop 9 microgrids, primarily for the purpose of maintaining power in critical buildings during power outages.[258] This initiative came into action as a result of Superstorm Sandy, in which 458,000 people in Connecticut were without power as a result of the storm.[259] While Connecticut took action to develop the Smart Grid and microgrid technology, New Jersey is perhaps a better example of federal and state cooperation to develop a microgrid system.

Beginning in 2013, the Department of Energy has joined New Jersey to establish an advanced microgrid system primarily with the purpose of insuring the transit system. Governor Christie explained, "This first-of-its-kind electrical microgrid will supply highly-reliable power during storms, and help keep our public transportation systems running during natural times of disaster, which is critical not only to our economy, but also emergency and evacuation-related activities."[260] This, in concert with Connecticut, is prioritizing critical infrastructure to set a precedent for further development, and is a perfect example of federal and state cooperation to develop a more reliable electrical grid.

In addition to the $40 million previously mentioned, New York is taking even further measures than either Connecticut or New Jersey. In January of 2014, Governor Cuomo announced a $17 billion program to "transform New York's infrastructure, transportation networks, energy supply, coastal protection, weather warning system and emergency management to better protect New Yorkers from future extreme weather."[261] The $17 billion is a combination of state and federal funding, furthering the notion that splitting the cost is the more effective means to accomplish development. [262]

Cooperation between the state and federal governments, as well as local entities is important. The cost of implementing this technology is tremendous, and splitting the cost can divide both liability and potential benefits. In addition to the cost burden, cooperation is essential because the federal government has the means and local and

---

[258] "Gov. Malloy Announces Nation's First Statewide Microgrid Pilot." *Daniel P. Malloy: Governor of Connecticut*. July 24, 2013. http://www.governor.ct.gov/malloy/cwp/view.asp?A=4010&Q=528770. Retrieved June 20, 2014.

[259] http://www.cbsnews.com/news/superstorm-sandy-more-than-7-million-without-power/

[260] "Energy Department Partners with State of New Jersey to Study Ways to Improve the Reliability of New Jersey's Transit System in Aftermath of Superstorm Sandy." *Energy.gov*. August 26, 2013. http://energy.gov/articles/energy-department-partners-state-new-jersey-study-ways-improve-reliability-new-jersey-s. Retrieved June 20, 2014.

[261] "New York Earmarks $40 Million for Ten Microgrid Projects." *Microgrid News: Homer Energy*. January 10, 2014, http://microgridnews.com/mn1-10-14-1.htm. Retrieved June 20, 2014.

[262] "Governor Cuomo Announces Broad Series of Innovative Protections; Vice President Biden Credits Governor Cuomo's Storm Plan as A Model for Future Recovery Efforts." *Governor Andrew M. Cuomo*. January 7, 2014. http://www.governor.ny.gov/press/01072013-cuomo-biden-future-recovery-efforts. Retrieved June 20, 2014.

state entities have the specific knowledge. This is an undervalued asset of cooperation, as the effectiveness of state and local organizations is overlooked. The states possess the ability to play a unique role in the development and implementation of Smart Grid and microgrid technology; and we should look to New York, New Jersey, and Connecticut as potential test beds for a precedent.

## INFORMATION SHARING

The issue of information sharing is a notable point regarding the relationship between the public and private sector. As previously discussed, cooperation is important, and information sharing is integral to the success of this cooperation. Understandably, sensitive information is often at the root of a risk, and this makes it difficult to discern between information that needs to be shared and what information needs to remain confidential.

Again, as described before, the development of the tear line process and the information provided to state and local authorities—alongside the utility industry—is vital to grid security.

Creating a network of information systems to facilitate an efficient flow of information between federal, state, and local governments, state and local law enforcement, and utility operators is essential to determining which information is shared and which is withheld. This network would need to be implemented in tandem with simplified classification standards, improved access to security clearances, and adequately trained personnel. A stable network controlling the flow of information could prove to be the most effective means of filtering information, as well as relaying vital intelligence rapidly. The ideal grid would be one that provides for the instantaneous, automated isolation of an affected system and subsequent rerouting of network traffic and electric power to minimize disruption. In order for such systems to effectively operate, machine-to-machine sharing of information and threat signatures must be facilitated.

Information sharing is important due to the pressing threat of both cyber and physical attacks on utilities. For this reason, it's notable that the quality of information is infinitely more important than the quantity of information. Big Data can be important, but it's only useful if analytics software can turn the data into "actionable business

intelligence."[263] An overload of information with the intention to inform could do just the opposite. Scanning through excess information carries potential for overlooking the vital information as well as confusing certain information.

Utilities are not in a position to determine the severity of threats, and being provided with an over-abundance of information could lead them to wrong judgments. The utilities must not be bothered with unnecessary information, making the information sharing system closer to a "need to know" system. Essential information must be shared while unimportant information must be filtered out, but how is all the information gathered? States and organizations have started testing some grid analytics solutions, namely voltage optimization, asset management, and outage management. [264]

New software solutions have also been implemented to both monitor and analyze the grid. For example, PowerLogic ION EEM monitors the grid's electrical output and control systems, using analytics to monitor risk and prepare for and remedy possible threats.[265] These analytics also serve to increase both the efficiency and the reliability of the grid system as a whole. As can be expected, these solutions need financing to succeed on a larger scale. This includes investments in computers and other technology, as well as a trained labor force that can operate the monitoring systems. The Utility Analytics Institute spent $0.5 billion on analytics in North America in 2011, and is projected to have spent $2 billion by 2016.[266]

Additionally the growth of analytical software systems—such as those provided by companies like Palantir Technologies—allow for quicker, more automated information sharing through more intuitive user interfaces. These systems can also be used to automate the protection of private or personal information, thus addressing concerns about privacy and civil liberties. They can also provide a record of what information is accessed and by whom, so that malicious use of collected data can be investigated.

---

[263] "Data analytics buying guide part 1: What's in Big Data for you?" *Smart Grid News,* November 5, 2012, http://www.smartgridnews.com/artman/publish/Delivery_Asset_Management/Data-analytics-buying-guide-part-1-What-s-in-Big-Data-for-you-5253.html#.U6g_cbdOUdU

[264] Jeff St. John. "Soft Grid 2013: From Big Data Potential to Real-World Value." *GreenTech Media*, September 24, 2013, http://www.greentechmedia.com/articles/read/soft-grid-2013-from-big-data-potential-to-real-world-value. Retrieved June 23, 2014.

[265] "How do Electric Utilities Manage Energy?" *Schneider Electric.* 2009. http://www.powerlogic.com/literature/3000HO0831_IONEEMUtil.pdf. Retrieved June 23, 2014.

[266] "Data analytics buying guide part 1: What's in Big Data for you?" *Smart Grid News.* November 5, 2012. http://www.smartgridnews.com/artman/publish/Delivery_Asset_Management/Data-analytics-buying-guide-part-1-What-s-in-Big-Data-for-you-5253.html#.U6g_cbdOUdU. Retrieved June 23, 2014.

Ultimately, information sharing is only as good as the intelligence that is obtained. These new technologies can help by improving the collection of information, categorizing and analyzing it, protecting sources, methods, and personal information, and most importantly, providing information that is timely and pertinent to the entity best equipped to mitigate the threat. The information gathered must be filtered out to prevent a "drinking from the fire hose" situation in which the utilities and/or local authorities are overwhelmed. Additionally, as cyber threats continue to multiply and many utilities find it difficult to fully staff their security departments, personnel must prioritize which networks are the most critical at both the corporate and control systems levels. By doing so, emphasis is placed upon those vulnerable networks and utilities can obtain the most pertinent information that can be quickly analyzed and disseminated throughout the utility. This concept ties back to the tear line—a concept that should be a primary consideration when discussing information sharing.

Vertical and horizontal information sharing can be a useful tool to increase efficiency. It's important to understand that every decision or solution does not have to originate from the federal government and trickle down to local authorities. State and local government can create innovative solutions to problems on their own, and requiring top-down initiatives significantly limits how efficiently action can be taken.

This is not to suggest that state and local governments should not ever consult the federal government, rather they should consult the federal government when it will truly increase the effectiveness and efficiency. The federal government has many more resources at their disposal, and this can help the state and local governments with both resources and information. As expressed, the primary need for information sharing is the prevention of incidents. The best way to do this is to share intelligence regarding potential threats to the grid or utility company itself.

Federal, state, and local law enforcement play the largest role in this. Federal agencies—notably the FBI's InfraGuard program, which works in concert with the existing critical infrastructure sectors, the Department of Homeland Security, and local law enforcement—already have access threat intelligence and experience sharing information with state and local law enforcement and utility providers. Communication in all forms is the foundation for information sharing, and communication between law enforcement at every level and utility companies can be instrumental in securing the power grid and preventing an incident.

# INDUSTRY ACTION

Because of the dynamic and complex nature of grid security, waiting for executive or legislative action at any level—federal or local—is not feasible for utilities. Private industry has begun taking the initiative, developing innovative solutions to issues surrounding security, information sharing, and liability protection. While utilities can only do so much without the weight of law on their side, the steps they have taken are both commendable and necessary to continued improvement of grid security. In doing so, utilities recognize the importance of their public role and show, via action, that security and the bottom line are not at odds.

As stated in previous sections, information sharing is both critical to grid security and one of the most controversial issues discussed in the electric and cyber sectors. Utilities have proven again and again their interest in information sharing, recognizing that without cyber or physical threat information, they will be unprepared to handle attacks. At the same time, industry cannot agree with government on the best ways to facilitate information sharing in a way that protects utilities from antitrust violations. Recent statements have dismissed the problem of antitrust in cyber threats, but the liability concern remains, inhibiting potential industry expansion of information sharing.

Industry security concerns do not only exist in relation to external vulnerabilities, but also cover issues related to internal weaknesses of the system and the workforce. The way the grid system is set up affects how well it can respond to threats. Similarly, the system set-up affects worker satisfaction. Dissatisfied workers can regrettably become an insider threat, as they have the access to carry out physical attacks or even cyberattacks through, for example, an infected USB. Utilities can take the initiative to build up system strength and personnel screening to protect themselves from this internal threats.

Of course, what one utility does in response to internal and external threats may not be the solution for another. There is significant variation in utility size, type, and structure. What utilities in Manhattan, Kansas, need is not the same as what utilities in Manhattan, New York, need. As in legislation, adopting a one-size-fits-all approach in industry action is counterproductive. Additionally, electrical grids do not operate in isolation, but rather in connection with other utilities such as water, gas, and telecom. The environment an electric utility is operating within changes how it should approach threats. Recognizing both this heterogeneity and interconnectedness can lead to more flexible and successful grid solutions.

## PRIVATE SECTOR INFORMATION SHARING

From an industry perspective, it is critical to establish effective information sharing channels among utilities and between utilities and government. A utility in San Jose, California, may face the same threat that a utility in Des Moines, Iowa, faced a year previously, but the Californian utility cannot benefit from that experience if there is no established channel of communication between those two utilities, either directly or through federal agencies. Liability and antitrust issues need to be addressed before information sharing can expand, but once these concerns are settled, more information can be shared through clearer, automated systems.

Private industries' innovations are limited by their concerns about information sharing. Many industries believe—with good reason—that under the rigid antitrust laws sharing threat information is an example of collusion, opening them up to lawsuits and penalties for antitrust violation. Fear does not breed creativity, meaning these liability concerns have been detrimental to utilities' development of new methods of information sharing.

Legislation has not sufficiently addressed this concern, creating unnecessary ambiguity for utilities. While most recently introduced legislation has tried to include at least some liability protection, the limits of these protections have been heavily critiqued. While legislation will add weight and credibility to current conversations and statements about liability, the current congressional climate regarding cyber and grid legislation does not promise any comprehensive liability protection in the near future. Utilities must look elsewhere, then, for reassurance that cyber threat information is shareable.

That's where the Department of Justice comes in. In a joint statement with the Federal Trade Commission in April 2014, the DOJ stated that antitrust issues should not be a "roadblock" to cyber threat information sharing. According to the statement, cyber threat information is "very different" from the "competitively sensitive information" that would violate antitrust laws. So far, it is unclear what effect this statement has had on mitigating industry concerns, but it is at least a step in the right direction of relaxing rigid antitrust standards in favor of critical infrastructure protection.

Despite liability concerns, some initiatives are already underway to develop new automated systems of information sharing. Federal agencies and utilities have worked together to automate these systems, as effective automation would cut down on inefficient labor costs at both ends. Two of the most promising of these initiatives are

the Trusted Automated eXchange of Indicator Information (TAXII) program and the Cybersecurity Risk Information Sharing Program (CRISP).

TAXII is an example of development primarily spearheaded by the government. DHS produced TAXII as a way to "simplify and speed the secure exchange of cyber threat information." Once developed, the system has been gradually rolled out and implemented by industry.

On the other hand, CRISP had heavy industry involvement from its earliest phases. It was created as the result of collaboration between utilities, the Department of Energy, and national labs. CRISP is designed to provide "a near-real-time capability for critical infrastructure owners and operators to share and analyze cyber threat data and receive machine-to-machine mitigation measures." Still a pilot program, CRISP's popularity is growing as more and more utilities begin implementing it. Its reception by the grid and cyber communities is proof of the critical role industry plays in developing technology that is directly applicable to day-to-day utility operations.

## SECURITY OF SYSTEMS & PERSONNEL

While grid security often focuses on external threats to the grid, expecting cyber and physical attacks to come from the outside, internal threats are just as dangerous. This insider threat can potentially be mitigated by adjusting the architecture of the system itself and maintaining high standards for personnel screening. Both actions must come from industry because there is such variation in system architecture and personnel across utilities. Theoretically, each utility will have a better understanding of its own unique insider threats, leading to better preparation and crisis management.

The way a utility system is structured affects how it responds to threats. While each utility is (and probably should be, based on the different types discussed later) structured differently, there are some standards or guidelines in the electric sector that utilities should follow. One set of guidelines is the ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model), a White House initiative that the electric power industry collaborated on with DOE and DHS. ES-C2M2 provides a model of "industry-vetted cybersecurity practices," as well as an evaluation tool that allows utilities to compare themselves to the model.

Additionally, the NIST Cybersecurity Framework attempts to connect relevant groups across sectors and promote the best practices in cybersecurity. The foundation of these best practices is meant to be adaptable, industry non-specific, and risk-based. This

"living document" can be used by regulatory bodies, utility operators, and federal agencies to develop, guide, assess, or improve their comprehensive cybersecurity programs and security methodologies. Using these protocols can improve utilities' systems internally in order to protect against external threats.

This architectural structure can open doors for a potentially more dangerous hazard: the insider threat that comes from personnel. Often disgruntled employees, these risky personnel have greater access to the system and therefore greater power over it. This power can come in the form of cyber, such as an infected USB, or physical, such as destroying a critical piece of machinery. Such attacks can often be untraceable because there is no evidence of breaking into the system.

There are many examples of this threat, and even more that for obvious reasons have never been released to the press. Many instances are simply unhappy employees lashing out, purposely attacking the grid system. Others, though, are inadvertent, as employees are sent infected emails or given infected thumb drives by attackers, leaving the employee(s) to unwittingly harm the system. Intentional attacks are an issue, too, as DHS warns utilities that terrorists can easily gain insider access to the grid and conduct a cyber or physical attack from the inside.

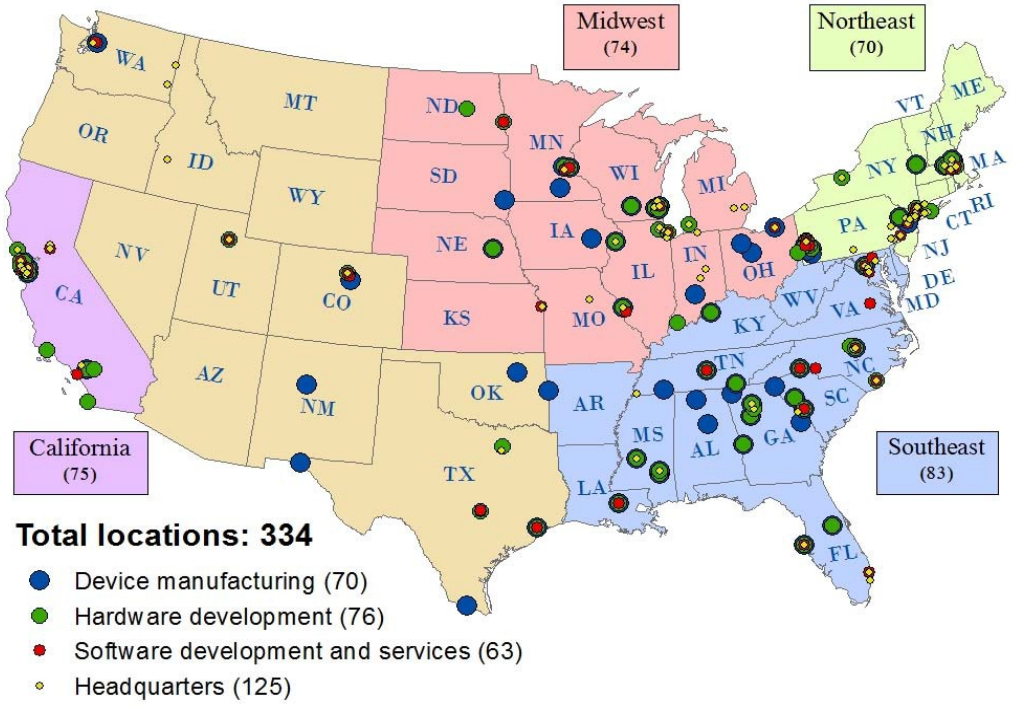
While the insider threat will never be eliminated, it can be mitigated by instituting regular personnel screening protocols. Utilities have already instituted some measure of personnel screening, but strengthening and improving this screening is necessary to risk mitigation. Increased screening may erode trust between employers and employees, as if employees were being accused of crimes they had not committed, but that is a necessary risk. Even the best, most loyal employees can unintentionally carry viruses that can harm the grid.

It is also necessary for personnel screening and changes to the system's architecture to be primarily an industry-led initiative. The executive branch can issue some kind of executive order or policy directive that instructs industries to incorporate this screening somehow, but the actual implementation falls to utilities. The variation in utilities' structures and needs affects how they can and should implement such a system.

## NOT ONE-SIZE-FITS-ALL

There are approximately 3,500 industries in the United States,[267] and they all have different needs, capabilities, and strengths. Because of this, these different utilities may face different threats, and even when they face the same threats, the necessary solutions may differ widely. Across-the-board initiatives, then, can only do so much good. A utility's geographic location, size, and type affect how it addresses problems of grid security, strengthening the idea that some of the most applicable solutions are industry-led.

In terms of location, it has come up again and again in roundtables that the security needs—and security capacity—of major investor owned utilities are vastly different than those of rural cooperatives or small municipal utilities. To some extent this is also a matter of size and type of utility, but place and culture are just as important. The figure below, compiled by Duke University researchers, shows a snapshot of leading firms and developers of Smart Grid technology. While this landscape changes regularly, the map below, which indicates only two centers in Kansas and uncountable numbers around San Francisco and New York City, is still indicative of existing




[267] "U.S. Electric Utility Industry Statistics." *American Public Power Association*. 2014. http://www.publicpower.org/files/PDFs/USElectricUtilityIndustryStatistics.pdf. Retrieved June 30, 2014.

patterns.[268]

Additionally, utility size is critical to the understanding of a utility's strengths and vulnerabilities. Some utilities serve a few hundred people, while others serve millions.[269] The size of a utility is not categorically "good" or "bad;" instead, it just changes the threat landscape. Smaller utilities may have fewer resources to protect themselves against attacks, but they also may be less vulnerable, and they could be less of a target for external attacks. On the other hand, large utilities could have more resources and advanced technology, but, resultantly, bigger vulnerabilities. This variation further emphasizes that a single method of grid security is likely not applicable in every utility.

Aside from size, there are three main types of utilities: municipalities, cooperatives, and investor-owned utilities (IOUs). Municipal utilities are publicly-owned and provide power to all of a city's residents. IOUs, conversely, are privately-owned for-profit utilities managed by a board of trustees. Cooperatives are somewhere in the middle, as they are non-profit enterprises owned by customers who all have an equal say in utility management. Cooperatives are most frequent in rural areas not covered by IOUs.[270]

## LINKS WITH OTHER INDUSTRIES

Whether they like it or not, all the major critical infrastructure providers are interconnected and interdependent. When a natural disaster occurs, such as Superstorm Sandy or the 2012 Derecho, damage affects all critical industries, from electric to water, telecom, and gas. As many roundtable participants have argued, among critical infrastructure sectors, the grid is the "most critical of critical." This applies in the case of natural disasters, too. Water, telecom, and gas utilities all rely on electricity to function. When the grid goes down, everything later on in the supply chain goes down. Inter-industry information sharing, communication of best practices, and wide-spread threat preparedness is necessary, as all major utilities benefit from the strength of the electrical grid.

---

[268] Marcy Lowe, Hua Fan, and Gary Gereffi, "U.S. Smart Grid: Finding new ways to cut carbon and create jobs," *Center on Globalization, Governance & Competitiveness, Duke University,* April 19, 2011, http://www.edf.org/sites/default/files/smart-grid-cut-carbon-create-jobs.pdf. Retrieved July 2, 2014.

[269] "Form EIA-826 detailed data," *U.S. Energy Information Administration,* March 2014, http://www.eia.gov/electricity/data/eia826/. Retrieved June 30, 2014.

[270] "Types of Electric Utilities." *Iowa Energy Center.* http://www.iowaenergycenter.org/iowa-electric-utility-structure/types-of-energy-utilities/. Retrieved June 27, 2014.

For example, after the 2012 Derecho, over 100 Washington Suburban Sanitary Commission (WSSC) facilities in the D.C. metro area were left without power. Lack of electricity meant the water treatment plants were unable to keep functioning, affecting WSSC's 460,000, customers in Montgomery and Prince George's counties.[271] The water industry cannot do its job without electricity, so it is in its best interest to support measures to secure the grid.

Telecom industries faced similar dangers after the 2012 Derecho. In the Virginia, Ohio, and West Virginia area, the storm took down 77 emergency call centers and left 2 million people unable to call for emergency services.[272] Lack of telecommunication then means emergency responders cannot do their job, either, as they may have no way of knowing who is in need of assistance. It is necessary to have an infrastructure in place at all times, although especially in the wake of natural disasters, that can provide power and electricity to those industries that greatly need it.

Like water and telecom services, the gas industry suffered without power after a natural disaster. When Hurricane Sandy raged through the Atlantic in 2012, New Jersey Natural Gas endured extreme damage that took more than a year to repair.[273] Power outages contributed to the utility's weaknesses, both directly and indirectly in the way it affected telecommunications.

These natural disasters, like other cyber or physical attacks, create domino effects that span well past the electric sector. Industry initiatives to secure the electrical grid do not need to originate solely in the electric industry. Effective information sharing channels or methods of communication established by water or gas industries could be adapted to the grid. This sharing of best practices would not constitute antitrust violation, and even the sharing of sensitive threat information among industries would be reasonably protected under the DOJ/FTC statement discussed earlier. Improving the grid benefits everyone. Industry interdependence must be seen as a valuable asset, not an obstacle.

---

[271] Kate S. Alexander. "Montgomery County wants WSSC to plan for power outages." Gazette.net. October 3, 2012. http://www.gazette.net/article/20121003/NEWS/710039841/&template=gazette. Retrieved June 30, 2014.
[272] Roger Yu. "FCC blames phone companies for Derecho 911 outages." *USA Today*. January 10, 2013. http://www.usatoday.com/story/money/2013/01/09/fcc-derecho-911-outage/1821695/. Retrieved June 30, 2014.
[273] David P. Willis. "Sandy less costly for N.J. Natural Gas than was feared." USA Today. February 8, 2013, http://www.usatoday.com/story/money/business/2013/02/08/sandy-natural-gas-utility/1902439/. Retrieved June 27, 2014.

## MANAGEMENT MODELS: COORDINATING CSOS & CISOS

As the number and severity of threats to the grid increase, it is especially essential for all security-related management and task forces to be on the same page. This primarily refers to the interaction that CSOs (Chief Security Officers) and CISOs (Chief Information Security Officers) of utilities have with each other and with other members of the management team. Stronger management, in terms of information and communication, is better prepared to deal with emergency situations.

The convergence of IT (information technology) and OT (operations technology) is part of this broader coordination. Because IT and OT are both growing more sophisticated, interpretation of new technology and information depends on an understanding of both sectors. IT-OT convergence and collaboration can improve efficiency, increase information sharing, and mitigate security risks.[274] A divide-and-conquer mentality to the grid only goes so far; collaboration is growing increasingly necessary to developing a holistic view of how grid security can be addressed.

One example of such coordination is EEI's Threat Scenario Project, which identifies major threats to the grid and possible methods utilities can use to mitigate these threats. David Batz, director of the Cyber & Infrastructure Security at EEI, said the purpose of the project is "to continue an engagement between the CEO, the CFO, the chief security officer [and] the chief information officer to say where are we doing well, where are we doing less well [and] what makes sense in terms of resource allocation." [275] Because EEI understands the amount of variation in utilities, its suggestions are as much about what utilities can implement as they are about encouraging further discourse within management about security threats.

---

[274] Tim Taylor, "IT-OT Convergence: Breaking down silos to achieve a more enabled workforce and more informed stakeholders," *Fortnightly*, February 2013, http://www.fortnightly.com/fortnightly/2013/02/it-ot-convergence. Retrieved July 2, 2014.
[275] Corina Rivera-Linares, "EEI: When it comes to cybersecurity threats, 'This is not your parents' utility anymore,'" *Energy Biz,* December 7, 2012. http://www.energybiz.com/article/12/12/eei-when-it-comes-cybersecurity-threats-not-your-parents-utility-anymore. Retrieved July 2, 2014.

# FINANCIAL & INSURANCE INCENTIVES

The private sector's financial and insurance sectors have a significant role to play in incentivizing both grid security and innovation. At a time when all levels of government—federal, state, and local—are confronted with limited resources, partnerships with the private sector and legislation aimed at creating private sector incentives can answer key grid challenges.

The insurance and reinsurance industries have a vital role to play in modeling risk, identifying threats and vulnerabilities that clients face, and encouraging best practices that mitigate these risks and speed recovery. Smart grid innovations will also allow insurers to utilize vast streams of data also available to utility operators—allowing for enhanced modeling and risk monitoring.

In the overall market, due to a convergence of factors—including slowing economic growth; rising electricity prices; an increase in government programs incentivizing developing technology; falling costs of distributed generation and Distributed Energy Resources (DER); and an enhanced focus upon implementing DER—it is clear that the current utility business model (cost-of-service regulation) faces significant challenges in the 21st century. This challenge becomes even more significant as new technologies disrupt the existing business model paying for their implementation.

The alternative model, known as Results-Based Regulation, provides utilities with the ability to develop long-term revenue plans that includes investment in and implementation of new technologies and/or methodologies. Using such models, both utilities and their investors can have a stable environment for determining key security and reliability benchmarks, especially as generation and distribution models change with technological innovation.

These modernized cost recovery models—largely implemented at the state and local level—incentivize outside investment in utility improvements alongside the cost recovery for significant security improvements. Combined with insurance incentives—to be discussed in further detail below—this creates a framework for outside investors to provide additional funding for major infrastructure upgrades and innovation. Additionally, these frameworks will allow municipal utilities and cooperatives to improve their security and infrastructure.

## THE ROLE OF INSURANCE COMPANIES

As multiple threats confront the security of the electrical grid, the insurance sector within the United States has a unique and important role to play in addressing these challenges. Insurance companies are currently leveraging advancements in grid technology to promote certain behaviors and utilize the data made available. As private sector partners to the grid, insurers can provide market-based incentives that are based in insurers' experience in risk modeling, threat analysis, and information sharing.

Historically, insurers have been concerned by the threat of disruption to the traditional top-down generation, transmission, and distribution system, which could result in a widespread blackout or cascading failure. By increasing redundancy and reliability throughout the grid, through the implementation of Smart Grid and microgrid technology, the overall risk to insurers decreases.

The insurance industry largely uses impact modeling to evaluate how to properly insure the electrical grid and to assist utilities in prioritizing components or practices, adapting threat mitigation postures, and the economic allocation of resources. These models—often using actuarial data—are based on experiences with past incidents, as well as simulations based on known risks. Thus it can be difficult for insurers and utilities to accurately model incidents—especially "Black Swan" scenarios—that have yet to occur.

Thus, while the insurance industry has a significant amount of modeling and actuarial data regarding severe weather and similar physical events, there is little in the way of actuarial data to model the impact of a major cyberattack or EMP/GIC event. Additionally, events such as a terrorist attack or other events that involve variability of the behavior or strategy of an individual or group are difficult to model.

Through the insurance underwriting process, the expertise of insurance underwriters, and more flexible premium structures—where allowed by regulation—can also incorporate auditing of security procedures and frameworks. While government entities—notably FERC—already conduct cybersecurity and other security audits, insurance processes and premium models—if provided with sufficient data by utilities—can also provide positive incentives for adopting best practices outside of the perceived heavy hand of regulatory action. If portions of the grid operation or utility infrastructure are classified, insurers will need to go through clearance processes as well to carry out this process.

Additionally, as part of the insurance models, these processes can leverage tools and experience from across the insurance industry and utility sector for securing more complex and/or networked systems, which can be vital for security preparation and incident response for smaller utilities. As more electrical utilities adopt insurance plans, it should not deter those utilities from continuing to implement or invest in cybersecurity or physical security technology or methodologies. Additionally, smaller utilities can benefit from some of the resources provided by the insurance industry in terms of both security preparation and incident response. Finally, as the grid—along with many other sectors of society—begins to increase in connectivity and collect large amounts of data, insurance companies will seek to harness these data streams to improve modeling, monitor operations, and analyze risk. Smart grid technology will be key to improving the resolution of these models, and insurers will work alongside utilities to better understand the data and resulting trend analysis made possible by the installation of smart systems.

## CHALLENGES TO CURRENT BUSINESS MODELS

The current model is highly regulated by state commissions, which set fixed rates upon a cost-of-service model. If these standards are not met, utilities must pay significant financial penalties. Adopting new technologies and remedying grid vulnerabilities requires—in many cases—a reexamination and reform of existing regulatory structures and political attitudes.

Additionally as new technology is implemented—be it Smart Grid, electric vehicles, solar panels, wind turbines, or future technological innovations—utilities face the challenge of maintaining rising technological integration costs in an environment where falling energy costs result in lower revenues. As a result, a future business model would have to integrate new ways or revise current ways that utilities fund technology through tariffs or net metering. Overall, the rates of a majority of "electric distribution companies continue to be set under a model focused on the utility's cost of service rather than on delivering value to customers."[276]

An alternative to the current business model for utilities is Results-Based Regulation. Ultimately, this model is designed to support utility investment in new technology; provide incentives for innovation and performance; and to encourage utilities to deliver

[276] " GE: Time to Rethink Electric Utility Regulation," *GE*, Oct. 22, 2013, http://www.gedigitalenergy.com/press/RethinkRegulation/index.htm

long-term value to customers. The key component of this model is a multi-year revenue plan that can be based upon an assessment of future costs rather than current costs. By doing so, utilities can adjust their rates according to changing business needs, which specifically incentivizes the implementation and integration of 21st century technology into the bulk power system.[277]

Within the results-based regulation model, utilities can begin to invest in technology to harden the grid against future threats and for the integration of new technologies such as Smart Grid and microgrid technologies. In addition, the Results Based Regulation model holds electrical utilities responsible for providing results from their investments. The financial and social accountability inherent in this business model will ensure that utilities invest in technology or methodologies that will provide customers with a reliable source of electricity.

California also provides key lessons about the integration of renewable energy sources, as legislative mandates have required their integration. Utilities have grappled with the high cost associated with funding solar photovoltaics (PV), geothermal energy systems, wind turbines, and electric vehicles (EV).

Thus the question has been how to reform the current rate structure to integrate renewable distribution and generation sources through either net metering or other tariffs. The current tiered rate structure, which is based upon energy usage, has fostered a large gap between low and high usage rates. Opponents of the tiered rate structure argue that lower income households, who do not have the financial ability to install this technology and rely upon utilities for energy, have a larger financial burden placed upon them.

Through a combination of a net metering program and infrastructure tariffs, customers will be able to sell excess energy back to their utility, which in turn will lower their monthly electrical bills. Utilities who have supported this practice believe that it could assist as a funding mechanism to pay for the integration of new technology and distribution system upgrades.[278]

As California continues to provide an example through its imposition of performance metrics, the state and its utilities must formulate how to measure other standards,

---

[277] Paul a. Centolella & David Malkin, "Results-Based Regulation: A Modern Approach to Modernize the Grid," Oct. 23, 2013, http://www.gedigitalenergy.com/regulation/#data_viz

[278] Kay Stefferud, "Hope at last? California offers net metering compromise," *SmartGrid News,* Oct. 11, 2013, http://www.smartgridnews.com/artman/publish/Business_Policy_Regulation/Hope-at-last-California-offers-net-metering-compromise-6096.html#.U0f6HahdVWI

including needed investments in, and incentives for, grid modernization and security. Doing so requires open and consistent dialogue between utility executives, technological innovators, energy regulators, and political leaders.

## BUILDING THE BUSINESS MODEL FOR THE GRID OF THE FUTURE

In addition to the question of modeling risk and insuring the electrical grid, how utilities recover costs continues to be a complex issue. Typically, there are three to four different entities providing electricity at the different stages—transmission, distribution, and generation—and currently, it is not clear where the monetary burden should fall. While traditional models of cost recovery would require increased rates for consumers, this would require action across fifty states and additional municipalities—such rate increases would likely create political challenges.

Additionally, with the shift to Smart Grid and microgrid technologies and the likely disruption of traditional top-down generation, transmission, and distribution models, there are questions about the traditional cost recovery and business models that would provide funding for security upgrades. A combination of private sector investment, increased user fees, smarter metering, and state/federal assistance for critical facilities is likely the ideal compromise. Further examination of the costs, benefits, and challenges of these alternatives is required by both industry experts and the policy community.

# THE FUTURE OF THE GRID

## ADDRESSING AGING INFRASTRUCTURE

There are multiple factors that negatively influence the safety and security of the electrical grid including—the age of components that comprise the grid, such as power plants, transformers, and transmission lines, many of which are over 25 years old. As threat actors become more advanced and the possibility of a joint cyber-physical attack increases, utilities must update the grid to deter 21st century threats. As the grid is modernized, there is an opportunity to bake security into the grid and its constituent components. However, it must be noted that as the grid is modernized and networked, the risk of cyberattack increases.

Additionally, the majority of transmission and distribution lines, along with generator step-up high voltage (HV) transformers and substation step-down HV transformers, are located above ground and in remote locations. Vital to our electrical grid, these stations serve as the "on ramps and off ramps," respectively, of the national electrical grid transmission system. These components are exposed to a variety of physical attacks and are exposed to weather-related events such as hurricane force winds, flooding, lightning, or falling trees. According to an analysis conducted by the *Wall Street Journal,* there were 274 instances of vandalism or deliberate damage to the electrical grid over the past three years.[279] Additionally, there were approximately 2,500 attacks against transmission lines and towers throughout the world in the past ten years.[280]

As the impact that aging infrastructure has on the security of the electrical grid is a common concern among utility personnel, the outsourcing of equipment is a vulnerability that utilities must face. High voltage transformers are an area of vital concern due to their size, the complexity of their manufacturing, and the lack of domestic production. As a result, electrical utilities, the National Labs, and federal government should focus on solutions for domestic production of key grid components and computer hardware.

As mentioned in multiple roundtable sessions, it is necessary for federal agencies to formulate reliability standards to protect the grid from various types of attacks. The

---

[279] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *Wall Street Journal,* Feb. 18, 2014, http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778

[280] *Terrorism and the Electric Power Delivery System,* National Academy of Science, 2012, http://www.nap.edu/openbook.php?record_id=12050&page=32

transmission components within the grid are regulated by both FERC and NERC, yet the distribution system is regulated on the state level. As a result, universal practices are not implemented, which has led to imbalances in security across the grid. According to statistics compiled by the Edison Electric Institute, approximately 90 percent of all power outages occur within the distribution system of the grid.[281] For utilities to sufficiently respond, mitigate, and recover from physical attacks, including weather-related events, it is necessary to focus on state-level regulations, as well as industry standards, for the distribution system of the grid.

## BUILDING THE SMART GRID

One of the ways utilities are updating the electrical grid is through the implementation of Smart Grid in 21st century technology. These advancements in technology range from fiber-optic cables, SCADA systems, Advanced Metering Infrastructure, in-home displays, meter data management systems, and Electrical Transmission and Distribution Systems. Considering the high cost of integrating this technology into the existing grid structure, the Department of Energy developed the Smart Grid Investment Grant (SGIG) Program, which provided funds to 99 projects throughout the United States. Smart Grid technology is a double-edged sword. Its fundamentally networked nature presents new vulnerabilities, yet the ability to better monitor the grid and its functions will improve efficiency and situational awareness.

As Smart Grid systems are being installed throughout the country, it is vital that the correct cybersecurity precautions are practiced. The two most important reasons for cybersecurity in the Smart Grid system are power system reliability and confidentiality and privacy of customers.[282] A utility can use Smart Grid to avoid or shorten power system outages so electricity is fully functional 100 percent of the time for customers and businesses. Additionally, the utility must ensure the confidentiality and privacy of its customers. Smart grid systems are being installed more frequently into homes and businesses, and energy consumption and regulation is becoming more accessible to customers.

---

[281] "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages," *Executive Office of the President,* August 2013, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf

[282] Ed Vard, "Key Cyber Security Purposes for the Smart Grid, *Electrical Engineering Portal,* April 12, 2012, http://electrical-engineering-portal.com/key-cyber-security-purposes-smart-grid

## PRIVACY & SECURITY CONCERNS

While the installation of Smart Grid inherently gives more control to the customer, it also opens up a new range of privacy concerns regarding increased access points and other cyber threats. Customer privacy within Smart Grid systems is a fairly new issue, so confidentiality and privacy of information is important as researchers find the best ways to implement comprehensive cybersecurity measures. Additionally, there is no universal set of cybersecurity requirements because each system is different; Smart Grid implementation is unique to each utility and locality in terms of needs, services and usage. In order to ensure stability within this multifaceted system, these variances must be understood.

Utilities currently possess—or are developing—several specific systems to deter and detect attacks on the electrical grid. Utilities have begun to integrate Software Management and Documentation Systems (SMDS) into SCADA systems. SMDS monitors all activities of the control system, assists IT and OT operators within an application restoration following any catastrophic event, and controls who may gain access to any SCADA application system. The SMDS also can develop Network Security Solutions, which range from firewalls to "Demilitarized Zones" to physical "air-gaps," which are all designed to prevent unwanted access to a network.[283]

Another defense-in-depth is the Virtual Private Network (VPN) tunnel, which ensures proper authentication and authorization of data transactions between networks. The VPN gives a utility private use of a public network through development of an encrypted tunnel between the server and the client; it is usually consistently safe, but due to variation between devices, there is some vulnerability. To fully secure a VPN from unauthorized access, a high level of authentication must be implemented in all networked devices.[284]

To detect any potential threats, many utilities have also invested in Intrusion Detection Systems (IDS). An IDS is implemented by utilities to recognize intrusions based upon different factors; it is often able to detect any unusual patterns of activity or communication attempted from an unauthorized address. The IDS creates a log of suspicious events that can also be manually inspected to determine true intrusions over false alarms.[285] Aside from deterrent and detection systems technology, physical

---

[283] "Cyber Security a Priority to Protect SCADA Systems," *Industrial Ethernet Book,* 2014, http://www.iebmedia.com/?id=9870&parentid=74&themeid=255&showdetail=true&bb=true

[284] Ibid.

[285] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems," *National Institute of Standards and Technology (NIST),* February, 2007, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

measures can also be taken to detect potential insider threats or attacks; this would include human detection measures such as behavioral analysis, background investigations, psychological profiling, and an analysis of individual motives.

In order to increase security, utilities and agencies must stabilize information sharing and private-public sector communication. There are several centers (Information Sharing Analysis Centers, Electricity Sub-Sector Coordinating Council, National Cybersecurity and Communications Integration Center at the Department of Homeland Security) that coordinate with local utilities to share alerts, indicators, threat actors, threat signatures, and information regarding previous attacks. Information sharing centers can be especially helpful in the case of extreme weather or a power outage; if a utility needed to shift a load to keep the lights on or obtain a spare transformer, for example, the utility could do this through contacting one of the information sharing centers. Mutual Assistance Agreements (MAAs) are also important in the wake of an event. They have a strong historical track record, and often encourage cooperation between different nations. However, with increased cyber incidents requiring computer hardware, software patching, and coding expertise, MAAs may not be the most effective way of eradicating the problem.[286]

Networked systems can also improve the dissemination of classified threat information between the federal government, state and local law enforcement, and utility operators. Information can be shared more efficiently by simplifying classification standards, improving access to security clearances, and hiring adequately trained personnel. Overall, there is a lack of legislation and public cause for concern regarding privacy and liability issues. This serves as a problem because it hinders the ability of the federal government to pass legislation that would regulate the information sharing process. The lack of legislation raises concerns amongst the private sector when it comes to sharing potentially useful information; much of the vertically shared information between a federal agency and a utility is classified, therefore, many operators within a facility are unable to access important information regarding recent attacks or potential threats.

Despite the lack of legislation, the Federal Trade Commission (FTC) and Department of Justice (DOJ) released an Antitrust Policy Statement on sharing cybersecurity information that is moving in a positive direction. The FTC and DOJ statements make it clear that properly designed cyber threat information sharing is not likely to raise

---

[286] Abraham Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, 2010, http://www.nap.edu/openbook.php?record_id=12997&page=179.

antitrust concerns, and that it can help secure the nation's networks of information and resources.[287] This was helpful for private businesses by making it clear that antitrust laws do not stand in the way of legitimate sharing of cybersecurity threat information.[288]

Smart grid technology presents a unique opportunity for automated, real-time, machine-to-machine information sharing that can react instantaneously—or even preemptively—to cybersecurity threats. However, it cannot be assumed that this information sharing technologies will be the panacea. Systems will continue to need qualified operators, combined with comprehensive intelligence, in order to defeat future threats.

## SMART GRID DEPLOYMENT

As Smart Grid technology has developed, several locations have emerged as leaders of the Smart Grid initiative. The Grid Modernization Index (GMI), released in 2013 by GridWise Alliance and Smart Grid Policy Center, ranked Texas and California as the top states succeeding in Smart Grid integration.[289] The top 15 states on the list all have three contributing factors in common: proactive efforts on cybersecurity and data privacy, investment from federal stimulus Smart Grid grants, and widespread Smart Meter deployment.

In Texas, Smart Grid efforts have been driven by retail energy choice. Due to its strong and competitive energy market, suppliers have offered flexible pricing systems and customer engagement programs. Additionally, increased Smart Meter penetration rates are credited with empowering customers to take advantage of services. A project setting the bar particularly high is the "Pecan Street" Mueller neighborhood project in Austin, Texas.[290] The project is being run by a $30 million initiative in collaboration with the Environmental Defense Fund (EDF), University of Texas, and Austin Energy. Almost every home in the neighborhood has installed Smart Meters, rooftop solar panels, and other Smart Grid devices. The initiative has led to the creation of the $1.5 million Pike Powers Laboratory, which is being built to research appliances, vehicles, air

---

[287] "FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information," *Federal Trade Commission,* April 10, 2014, http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity

[288] Ibid.

[289] Silvio Marcacci, "California and Texas Smart Grid Success Shows Way Forward for US," *Clean Technica,* 2013, http://cleantechnica.com/2013/07/22/california-and-texas-smart-grid-success-shows-way-forward-for-us/

[290] "Living Laboratory Shows How a Smart Grid Works," *Environmental Defense Fund,* http://www.edf.org/energy/building-smarter-grid-austin-texas

conditioners, and solar panels that will be necessary to complete the project.[291] The neighborhood's end goal is to noticeably increase efficiency, reliability, and security.

Another national leader in Smart Grid technology is the state of California. California is investing in the technology as a way of integrating renewables and moving toward a cleaner energy future. While several cities are implementing successful projects throughout the state, some worth nothing are the Anaheim AMI Project and the Irvine Smart Grid Demonstration. The Anaheim AMI Project is a city-wide deployment of advanced metering infrastructure (AMI) and other methods that will allow the city to manage, measure, and verify targeted demand reductions during peak periods.[292] For the Irvine Smart Grid Demonstration, Southern California Edison (SCE) is incorporating advanced Smart Grid technologies in an integrated system for the purposes of environmental and economic efficiency, safety, reliability and security.[293] It is installing Energy Smart Customer Devices such as smart appliances, solar systems, and photovoltaic (PV) solar systems. The project also includes the Year 2020 Distribution System, which will service advanced distribution equipment, smart metering, and renewable distributed generation. Throughout the process, the Irvine project has established a Secure Energy Network to manage telecommunication systems in what is claimed to be the safest and most secure way possible.[294] Participants in the roundtables highlighted the success of these initial pilot programs, yet they also shared their concerns about how regulatory models focused on existing technology—especially systems using serial communication—failed to recognize innovations in terms of security IP communication and other Smart Grid systems.

## THE ROLE OF NATIONAL LABS

The role of national labs has been vital towards developing technology aiding in the progression of Smart Grid systems and cybersecurity. Lawrence Livermore National Laboratory formed a five-year Research and Development program with Southern California Edison, Pacific Gas & Electric, and San Diego Gas & Electric to assist utilities by providing advanced computational and analytic capabilities and new platforms for

[291] Ibid.
[292] "California Smart Grid Toolkit," *Smart Grid News,* Nov. 12, 2012, http://www.SmartGridnews.com/artman/publish/Projects_Toolkits/California_Stimulus_Toolkit-720.html
[293] Ibid.
[294] Ibid.

workforce training.[295] The program was designed to focus on four key issue areas: security, workforce preparedness, operations, and resource planning.

While improving these issues, the lab is also researching cybersecurity risks, threats, tools, and methodologies to protect the electrical grid. The Sandia National Laboratories, operated by the U.S. Department of Energy and Lockheed Martin, have been working on measures to improve insider threat detection. The lab is in the process of upgrading cyber identity management and Insider Threat Monitoring through Ephemeral Biometrics (EB). EB is unique because individual identities are tied to living biometric data that is active and continuous.[296] The purpose of Sandia Lab's research is to create new, "outside-the-box" authentication techniques, such as alternatives to passwords.

The lab's research wants to develop methods that capture an individual's vital signs as part of the authentication process; by requiring a sensor bound to a person's identity worn around the neck or wrist to measure pulse rate, monitors could be certain it's always a genuine human requesting access. That sensor could also capture location data, eliminating possibilities of insider threats.[297]Another important research facility, the National Energy Technology Laboratory, is managing 60 Research and Development projects aimed at developing components of the Smart Grid system, such as high-temperature superconductors, energy storage, and cybersecurity.

The lab's goal is to modernize the grid, and warns that an extensive loss of the current grid would have significant, long-term repercussions. They are trying to achieve results similar to that of the "Fort Knox model,"[298] where an army post frequented by severe weather lost its connection with the local public power utility in 2009, leaving many of its buildings without power for up to 10 days. Fort Knox responded by creating a back-up power system that would be able to efficiently recover following an attack or power

---

[295] S. Julio Friedman, "Shaping California's Smart Grid: Employing the Best Computer Technology," *Energy Biz,* Jan. 2012, http://www.energybiz.com/magazine/article/251061/shaping-california-s-smart-grid

[296] "Ephemeral Biometrics: An Alternative to Traditional, Event-based Authentication," *U.S. Department of Energy,* June 4, 2014, https://www.fbo.gov/index?s=opportunity&mode=form&id=06e9abca57bdd9dac64902e39f039c4f&tab=core&_cview=0.

[297] Sung Choi and David Zage, "Ephemeral Biometrics: What are they and what do they solve?" October, 2013, https://www.cs.purdue.edu/homes/zagedj/docs/iccst2013.pdf

[298] Joe Miller, "What is the Smart Grid? Illinois Smart Grid Initiative," *National Energy Technology Laboratory,* June 2008, http://www.netl.doe.gov/File%20Library/research/energy%20efficiency/smart%20grid/presentations/ISGI-Orientation_Miller_APPROVED_2008_05_14.pdf

failure.[299] The Fort Knox model implements combined heat and power (CHP) systems to provide backup power and significant yearly energy savings at the base.[300]

## FEDERAL INVESTMENTS & GRANTS

In addition to the role of national labs and utilities, the federal government has been working to place the nation's energy security at a higher priority. This initiative was partially sparked by the Energy Independence and Security Act in 2007, and was followed by the Department of Energy's Smart Grid Investment Grant (SGIG) program. A result of the 2009 American Recovery and Reinvestment Act, the SGIG program rewarded 99 utility projects to implement new technology and practices. There are four main topic areas that the SGIG program has been zeroing in on to transform the electrical grid, which include the following: Electric Transmission Systems (ETS) such as line monitors communication networks, and phasor measurement units; Electric Distribution Systems (EDS), which include automated sensors and controls for switches, capacitors, and transformers; Advanced Metering Infrastructure (AMI), which includes communication systems, smart meters, and meter data management systems; and finally, Customer Systems (CS), such as in-home displays, programmable communication thermostats, web portals, and time-based rate programs.[301]

The purpose of SGIG is to accelerate the modernization of the nation's electric transmission and distributions systems, create tools and technology to increase flexibility and efficiency, and to promote investments in Smart Grid technology. The program has been successful in dramatically accelerating the deployment of Smart Grid technology, optimizing grid performance and reliability by using electronic data and intelligent devices, and improving resiliency to natural disasters—all while also maximizing economic efficiency. Successful projects have received federal financial assistance of up to 50 percent of eligible costs, for a total funding of $7.9 billion ($3.4 billion in federal grants and $4.5 billion from private donors) going toward improving the electrical grid. Smart meter deployment took up the largest percentage of these costs, as utilities all over the nation are making the simple, efficient switch to installing smart meters in surrounding homes.

---

[299] Dan Provost, "Using CHP to Bring Energy Security to Fort Knox," *Business Energy,* August 2013, http://www.distributedenergy.com/DE/Editorial/Using_CHP_to_Bring_Energy_Security_to_Fort_Knox_22722.aspx

[300] Ibid.

[301] "Smart Grid Investment Grant Program: Progress Report," *US Department of Energy,* July 2012, http://energy.gov/sites/prod/files/Smart%20Grid%20Investment%20Grant%20Program%20-%20Progress%20Report%2020July%202012.pdf

The SGIG program has sparked an increased awareness of grid operations, but has not necessarily directly addressed security issues. While smart meters improve efficiency and reliability, experts warn that the increased transition to smart meters and internet-based technology may also cause an increase in hackers.[302] The FBI warns that insiders and individuals with only a moderate level of computer knowledge are most likely able to compromise smart meters with readily available, low-cost tools and software.[303] Due to the fact that the SGIG project funds were awarded to several small utilities, the utilities' goals are often geared toward the customers and toward achieving decreased consumption costs, rather than ensuring security and defense. A utility in Fulton, Missouri, which was given a $3,055,282 budget by the SGIG program, has set a goal to implement smart meters and two-way communication for customers to view their consumption as well as implement time-based rate programs. The program's Smart Grid report does have a "Cyber Security and Data Privacy" section, but it is very minimal and the majority of the section focuses solely on customer information privacy.[304] As of now, there is no specified plan in the utility's Smart Grid handbook on what to do in the case of a real threat. Another recipient of SGIG funding, the Electric Power Board (EPB) in Chattanooga, Tennessee, has been using its funds to work toward the deployment of a fiber optic network as the primary means of communication for all Smart Grid equipment.[305] They hope to reduce power surges from frequent storms occurring in the Southeast. EPB is also investing in AMI, which will enable two-way communication with the smart meter.[306] This will be connected with the addition of energy management web portals, which will be helpful for customers looking to monitor and manage their energy usage. While these measures being taken will improve some security and energy efficiency, no statements were found in the new plan regarding emergency plans or specific security measures being addressed in the case of an event.

## SMART GRID & THE PUBLIC INTERNET

While Smart Grid initiatives have proven successful for improving efficiency, their reliance on wireless, "cloud," and Internet-based technology opens up a greater

---

[302] "FBI: Smart Meter Hacks Likely to Spread," April 12, 2012, http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/
[303] Ibid.
[304] "Missouri Smart Grid Report," *Missouri Public Service Commission,* Last updated February 14, 2014, http://psc.mo.gov/CMSInternetData/Electric/Missouri%20Smart%20Grid%20Report%20-%20February%202014.pdf
[305] "A Smarter Electric Circuit: Electric Power Board of Chattanooga Makes the Switch," *U.S. Department of Energy,* https://www.smartgrid.gov/case_study/news/smarter_electric_circuit_electric_power_board_chattanooga_makes_switch
[306] Ibid.

potential threat of hacking and cyber terrorism. The increased number of access points can be seen in Home Meters (smart meters) and customer interface, such as Home Area Networks (HAN) and Business Area Networks (BAN). Home meters, which send back information from the utility base to the home about how much electricity or gas is being used, are relatively new and may contain errors or open access points. Workers need to ensure that meters are secure, customer detail and privacy is protected, and denial-of-service attacks and infiltration by foreign intelligence services is prevented. Assessing the risks that come with smart meters is highly dependent on understanding what large networks they will be connected to,[307] and the design must permit errors to be easily fixed.

Customer interfaces which provide a connection between the utility and the customer through systems such as Home Area Networks (HAN) and Business Area Networks (BAN), have also contributed to the increased number of access points found in the electrical grid. Customer interfaces give the ability for the customer to connect devices within a home or business in order to receive detailed information regarding energy usage, as well as to help manage and monitor electricity usage.[308] They enable the communication and sharing of resources between computers, mobile, and other devices over a network connection. Components of customer interface include In-Home Displays (IHDs), Energy Management Devices, and Peripheral Devices. IHDs are essentially energy information displays; they receive real-time energy use data and help identify high-energy use appliances. Energy Management Devices are programmable communicating thermostats (smart thermostats), which allow the customer to program more settings. Peripheral Devices include gateways and range extenders that help communicate with smart meters to extend a signal.[309]

Companies and researchers are currently working on ways to improve understanding of Smart Grid and other electric-grid technology. One of the methods being focused on is data analysis. Data analysis is the science of transforming raw data into "real life" information to promote proactive decision-making. Data analysis can give businesses and utilities a comprehensive view of internal and external risks by alerting decision

[307] John Colley, "An opportunity for a secure digital society," *Computer Weekly,* http://www.computerweekly.com/opinion/Think-Tank-What-are-the-security-implications-of-putting-a-smart-meter-in-every-UK-home.
[308] "Home and Business Area Network Devices," *San Diego Gas & Electric,* http://www.sdge.com/residential/about-smart-meters/home-and-business-area-network.
[309] Ibid.

makers about potential fraud, unusual network traffic patterns, hardware failures, and security breaches.[310]

Companies such as GE, Siemens, Oracle, AutoGrid, Trove, IBM, and SAS have all begun to develop data analytic software to better understand and interpret Smart Grid technology. The three most widely implemented grid analytics solutions of data analysis have been voltage optimization, asset management, and outage management.[311] Information is analyzed in real-time, which helps heighten awareness of any problems within the grid.[312] San Diego Gas & Electric (SDG&E) has also emerged as a leader in the Smart Grid initiative. California's Title 24 Building Code requires all new thermostats, HVAC systems, networked lighting controllers, and automation systems in the state to come ready for two-way, automated utility-to-customer energy management.[313] SDG&E has been in the process of deploying 1.4 million smart meters. It has implemented a data management program through Itron and a customer web portal designed by Aclara; Itron and Aclara have assisted SDG&E in connecting with the consumer and with analyzing the large amount of data that has been collected by the smart meters.[314]

Utilities all over the nation have begun moving in the direction toward energy efficiency and reforming the electrical grid. In order to make a complete shift in this direction, one must understand the costs of implementing these measures. As previously mentioned, the Department of Energy has invested billions of dollars into the Smart Grid Investment Grant program. This is the biggest federal funding project for Smart Grid to date, as utilities are currently working on transforming regions with updates.

Additionally, venture capitalists have begun to welcome startup businesses looking to combat the rise in cybercrime. Chrysalix Energy Venture capital has taken on ReliOn, which is developing low-cost backup and remote primary power systems based on proprietary fuel cell technology; the company's goal is to back up utility SCADA systems to have stable and dependable telecommunications when natural and

---

[310] Jeff St. John, "Big Data on the Smart Grid: 2013 in Review and 2014 Outlook," *Greentech Media,* December 16, 2013, http://www.greentechmedia.com/articles/read/Big-Datas-5-Big-Steps-to-Smart-Grid-Growth-in-2014.
[311] Jeff St. John, "Soft Grid 2013: From Big Data Potential to Real-World value," *Green Tech Media,* September 24, 2013, http://www.greentechmedia.com/articles/read/soft-grid-2013-from-big-data-potential-to-real-world-value
[312] Ibid.
[313] Jeff St. John, "California's New Building Cod: a Grid-Smart Thermostat in Every Facility," *Green Tech Media,* April 3, 2014, http://www.greentechmedia.com/articles/read/californias-title-24-a-grid-smart-thermostat-in-every-building
[314] Jeff St. John, SDG&E's Massive Smart-Grid-to-Consumer Playbook," *GreenTech Media,* Dec. 19, 2011, http://www.greentechmedia.com/articles/read/SDGEs-Massive-Smart-Grid-to-Consumer-Playbook.

manmade disasters crash the electrical grid.[315] Venture capitalist Draper Fisher Jurvetson has taken on EnerNOC, which is a public provider of energy intelligence software (EIS) applications and technology for efficient Smart Grid use by energy users and utility and grid operators.[316] Additionally, GE Ventures is working with Trilliant, a Smart Grid solutions company. Trilliant provides utilities and energy retailers with Smart Grid initiatives, including transformer monitoring and grid load information for planning.[317]

Because of the potential pathways from the public Internet to the electrical grid—via the Smart Grid—grid security will involve not just utilities, but also the manufacturers of apps, appliances, software, and other systems/devices that connect to grid technology. With multiple entry points to the grid, it will be necessary to further analyze system architecture to make sure that there are not unsecured pathways from consumer devices or connections to the grid control systems. Additionally, security standards and software systems must recognize malicious activity—e.g. the simultaneous, wide-scale start or shutdown of power-intensive appliances, such as air conditioners, to create an imbalance on the grid—and respond to counter or isolate the activity and alert grid operators.

## COST RECOVERY & METERING

In addition to employing new research and development on the electrical grid, many are attempting to develop and campaign on new schemes for metering and cost recovery. The current "tiered rate" structure, which is based upon energy usage, has fostered a large gap between low and high usage rates. Cost-of-service regulation often faces significant challenges due to being highly regulated by state commissions, which set fixed rates upon a cost-of-service model. If standards are not met, utilities are required to pay financial penalties.

Currently, utilities face the challenge of maintaining rising technological integration costs in an environment where falling energy costs result in lower revenues. Edison Electric Institute, which represents investor-owned utilities, claimed that "disruptive technologies like renewables, efficiency, distributed generation and new storage innovations, will lead to declining power sales and therefore declining revenues."[318] Not only is this situation bad for business, but less revenue also provides less of a

---

[315] "Reli On," *Chrysalix Energy Venture Capital,* http://www.chrysalix.com/relion

[316] "Portfolio," *DFJ,* http://www.dfj.com/portfolio/index.php

[317] "Featured Companies," *GE Ventures,* http://www.ge.com/about-us/ge-ventures/portfolio-partners

[318] Peter Kind, "Disruptive Challenges: Financial Implication and Strategic Responses to a changing Electric Business," *Edison Electric Institute,* January, 2013, http://www.eei.org/ourissues/finance/documents/disruptivechallenges.pdf.

means for ensuring security measures. To address the problem, California utilities have created a system combining a net metering program and infrastructure tariffs. Customers will be able to sell excess energy back to their utility, which will in turn lower their monthly electric bills, while infrastructure and security costs can be recovered.[319]

Other utilities have decided to tackle the problem by embracing it and placing a greater emphasis on energy efficiency and renewables. Vermont's Green Mountain Power (GMP) has taken such an approach. Unlike most utilities, which are warning against profit-reducing energy models, GMP is establishing a new way of doing business through the solar energy model and net metering.[320] Called the "SolarGMP Initiative," GMP has already accomplished installing 26,000 solar panels in 1,000 days.[321] Through this initiative, it plans to create a more customer service-based business model.

Another potential alternative to the current business is Results-Based Regulation. This method would turn a cost-of-service model into a value-of-service model, as the idea would be to compensate utilities based on their ability to meet specified goals agreed upon in advance with regulators.[322] This model would be designed to support utility investment in new technology, provide incentives for innovation and performance, and to encourage utilities to deliver long-term value to customers.

## MICROGRID & DISTRIBUTED GENERATION

Interrelated to SmartGrid technology are microgrids, which are at their most basic form small-scale versions of the centralized electricity system. With the development of this technology, many states—in tandem with the private sector and federal government—have begun to implement both small and large-scale projects. In the wake of an attack or an extreme weather event, microgrids can provide electricity to the first responders and emergency services. Still, given the shift in architecture from centralized grids to

---

[319] Kay Stefferud, "Hope at last? California offers net metering compromise," *SmartGrid News,* October 11, 2013, http://www.smartgridnews.com/artman/publish/Business_Policy_Regulation/Hope-at-last-California-offers-net-metering-compromise-6096.html

[320] Tor Valenza, "Why a Vermont Utility CEO is Embracing Solar and Net Metering," *Renewable Energy World,* May 6, 2014, http://www.renewableenergyworld.com/rea/blog/post/2014/05/why-a-vermont-utility-ceo-is-embracing-solar-and-net-metering

[321] "Green Mountain Power Installs 26,000 Solar Panels in 1,000 Days," *Vermont Digger,* November 6, 2011, http://vtdigger.org/2011/11/06/green-mountain-power-installs-26000-solar-panels-in-1000-days/

[322] David Malkin and Paul Centolella, "Results-Based Regulation: A Modern Approach to Modernize the Grid," *GE Digital Energy* and *Analysis Group,* http://www.analysisgroup.com/uploadedFiles/Publishing/Articles/Centolella_GE_Whitepaper_Electricity_Regulation.pdf

distributed generation, questions remain about how the business model for this infrastructure will take shape.

## BUILDING MICROGRIDS

A microgrid is defined as a "conglomeration of small generation and loads that operate as a coherent system and connects to a wider grid as a single point load."[323] This is a very basic definition, as additional stipulations can be added to the definition when appropriate. These stipulations can include requiring the microgrid to have storage devices, maintain controllable loads, provide heat as well as power, and engage in island mode. Island mode is a state in which the microgrid disconnects from the main power grid and operates entirely in a disconnected state.

Currently, a microgrid has an operation capacity of roughly one gigawatt. This primarily comes from gas or diesel, as solar power currently consists of only three percent of operational generation. [324] There are several different areas to consider with regards to a microgrid, and these include technical, operational, and economic. The technical aspect covers voltage, power quality, frequency, and many other considerations. The operational considerations deal more with protection, security, load imbalance, and maintenance.

Finally, the economics of the microgrid consider cost, geographic dispersion, system life, and any other business related aspects. New microgrid technology has numerous benefits, ranging from broad to local. Perhaps the most notable of these benefits is the reliability of the microgrids, primarily due to their ability to operate independently. Other general benefits of the microgrid include improved efficiency and reduced emissions. Locally, benefits also include quality and reliability; but also a reduction in unwanted harmonics, a reduction in distribution losses, and the ability to combine heat and power. Yet, when investing in this technology, utilities should examine both the short and long term benefits of microgrids, including the possible disruption to cost recovery models and load balancing.

---

[323] Morris, Greg Young, Chad Abbey, Geza Joos, and Chris Marnay. "A Framework for the Evaluation of the Cost and Benefits of Microgrids." *Ernest Orland Lawrence Berkeley National Laboratory*.

[324] Munsell, Mike. "Solar and Other Renewables Are Key Inputs for Next-Gen Microgrids : Greentech Media." Greentech Grid. http://www.greentechmedia.com/articles/read/Solar-and-Renewables-Are-a-Key-Input-for-Next-Gen-Microgrids (accessed July 3, 2014).

## MICROGRIDS & RENEWABLES

In addition to the previously stated benefits, a microgrid system allows for a cleaner and more resilient grid. Microgrids are moving away from diesel towards solar, hydro, and wind-based power. There are a number of reasons moving away from diesel is positive progression, the most notable of which is environmental concerns. Burning diesel on a large scale is detrimental to the environment, but the environmental and logistical concerns, such as pipelines and transport vulnerabilities, with obtaining diesel cannot be overlooked either.

When experiencing utility outages, it is often difficult to transport diesel via road, rail, or pipeline to where it is needed—creating a self-perpetuating problem. Solar, wind, or hydro based power systems could be locally based and have the ability to store power, both of which would significantly increase the reliability of the grid.[325] Primarily funded by the Department of Defense and the Department of Energy, the SPIDERS program is making headway in the renewable energy microgrid field. SPIDERS stands for "Smart Power Infrastructure Demonstration for Energy Reliability and Security," and is headed by Sandia National Laboratories.

This $30 million project is to design 25 microgrids for military institutions throughout the United States. The primary objective is to both transition away from diesel and provide a more reliable grid. This project was successful, as tests show that the grids operate 90 percent on renewable sources. Projections suggest this will save $43,000 each year as opposed to an entirely diesel based system. Clearly, the SPIDERS program has shown that a microgrid can be cheaper, cleaner, and more resilient than a diesel based system. [326]

In addition to the Sandia National Laboratories initiative, other states and even independent institutions are developing microgrids based on renewable energy. One example is the University of California San Diego (UCSD). UCSD developed a microgrid that provides for 92 percent of the campus's electricity and 95 percent of the campus's heating and cooling. The microgrid uses both solar power, as well as wind power, and serves roughly 45,000 people on the UCSD campus. The university accomplished this through $8 million in independent donations, and the California Energy Commission has granted an additional $1.8 million to UCSD. The UCSD microgrid also proves the

---

[325] Casey, Tina. "In First Test, U.S. Military's SPIDERS Microgrid Uses 90% Renewable Energy." CleanTechnica. http://cleantechnica.com/2013/02/12/u-s-militarys-new-spiders-renewable-energy-microgrid/ (accessed July 3, 2014).

[326] Ibid.

practicality of the system, as the microgrid takes up about as much room as a tennis court. This is remarkable for a system that can provide heating, cooling, and electricity to 450 buildings—not to mention it's run primarily on solar and wind power. It's clear that the capability for a cleaner and more resilient grid is present, but implementing and organizing the system is where difficulty sets in.

## STATE MICROGRID PROGRAMS

Interrelated to the Smart Grid Investment Grant (SGIG) program are the advancements in distributive electricity systems, specifically microgrids, which have reinforced the reliability of the entire electrical grid. "The DOE estimated that as of 2007, there were more than 12 million distributed generation units installed across the United States, with a total capacity of 200 GigaWatts."[327] Microgrid technology has begun to rise in popularity, especially after weather events such as Superstorm Sandy. Due to the widespread and multi-day power outages that occurred after the October 2012 storm, many utilities have begun to evaluate how to reinforce and strengthen their distribution and generation systems specifically connected to essential public services.

With the expansion of this technology, many states in tandem with the private sector and federal government have begun to implement small and large-scale projects. Governor Cuomo of New York and Vice President Joe Biden recently announced the "Reimagining New York for a New Reality," which is a $17 billion dollar program aimed at modernizing the state's energy supply, emergency management, transportation network, coastal protection, and infrastructure. In addition to that program, Governor Cuomo also announced a $40 million dollar award through the NY Prize Competition focused upon building ten community-scale 'power grids' specifically for areas with 40,000 residents.[328]

Community-based programs have also been funded in both Connecticut and New Jersey. Nine microgrid pilot programs are scheduled to be implemented throughout the state of Connecticut, which total $18 million and are primarily funded by the Department of Energy and Environmental Protection (DEEP) Microgrid Pilot Program.[329]

---

[327] Richard J. Campbell, "Weather-Related Power Outages and Electric System Resiliency," *Congressional Research Service,* Aug. 28, 2012, http://www.fas.org/sgp/crs/misc/R42696.pdf

[328] "New York Earmarks $40 Million for Ten Microgrid Projects," *Microgrid News: Homer Energy,* Jan. 10, 2014, http://microgrid-news.com/mn1-10-14-1.htm

[329] "Gov. Mallow Announces Nation's First Statewide Microgrid Pilot," *Office of the Governor of Connecticut,* July 24, 2013, http://www.governor.ct.gov/malloy/cwp/view.asp?Q=528770&A=4010

Additionally, in August of 2013, N.J. Governor Chris Christie announced a $1 million dollar DOE program focused on implementing microgrid technology to the state's Northeast corridor transit system. This plan will assist in modernizing and adding new distribution and generation infrastructure to a transportation system, which serves approximately 900,000 customers per day. This specific project has been adapted from the blueprint developed by Sandia National Laboratories, which designed 25 microgrids for military installations throughout the United States.[330]

Additionally, Alan Rubacha, a senior project manager at a project based at Wesleyan University at Middleton, stated the grid will help to "achieve greater reliability, to provide additional emergency power in an outage, and to produce electricity for less cost with few emissions."[331] Wesleyan is spending $3.7 million for the microgrid to provide electricity, heating, and cooling to their athletic center.[332] Both the projects in Connecticut and New York are important to look at because they are pioneers with regards to the microgrid. It is clear at this point that microgrids are an invaluable tool, but small-scale success must be examined to pave the road for large-scale establishment.

The previously mentioned examples rely heavily on solar power for their microgrids. The SkyGrid Energy project in Hawaii, however, relies on wind power. Powered by an NPS 100 wind turbine, the Hawaiian microgrid has been fully functional since April 2013. While wind is the primary source of energy, a battery bank and inverter also contribute to the success of the microgrid. SkyGrid Energy generates approximately 200,000 kWh which is breakthrough technology for such a remote area.[333]

A variety of different microgrids can be successful, and geographic location must be taken into account. Hawaii is optimal for the wind turbines, whereas they wouldn't work as well in New York. An important aspect of the microgrids is the ability to store energy, as sun and wind are not predictable constants. SkyGrid Energy is a prime example of how a microgrid can adapt to and be successful in different environments.

---

[330] Magdalena Klemun, "DOE helps kick-start one of the first large civilian microgrid applications for New Jersey's hurrican-ravaged transit system," *Greentech Media*, Aug. 27, 2013, http://www.greentechmedia.com/articles/read/from-military-base-to-garden-state-nj-transit-plans-advanced-microgrid

[331] Kane, Brad. "CT Microgrid Program Seeks Full Financing." *Hartford Business Journal*. http://www.hartfordbusiness.com/article/20130318/PRINTEDITION/303149952/ct-microgrid-program-seeks-full-financing (accessed January 1, 2014).

[332] Gecan, Alex. "Gov. Malloy fires up state's first microgrid at Wesleyan." The Middletown Press. http://www.middletownpress.com/general-news/20140306/gov-malloy-fires-up-states-first-microgrid-at-wesleyan (accessed July 3, 2014).

[333] Northern Power Systems. "Remote Hawaiian Microgrid." . http://www.skygridenergy.com/pdf/Hawaiian_Microgrid_Case%20Study.pdf (accessed January 1, 2014).

## WIDESCALE IMPLEMENTATION

In the immediate future, microgrids are being used almost exclusively for critical facilities such as military bases, airports, and university or hospital campuses. This includes powering institutions such as hospitals and transportation systems. Especially with government funding, residential or even commercial microgrid establishment could not be justified. The technology for the microgrids needs to become more easily obtainable for residential and commercial use, and this doesn't appear feasible in the near future.

Specifically in New York, New Jersey, and Connecticut, the purpose of the microgrid is to ensure the reliability of the grid so that critical infrastructure can continue to operate throughout a power outage. This would have been invaluable throughout Superstorm Sandy, as outages could be localized and critical facilities would remain powered.

As previously discussed, the microgrid projects can be more effective when the cost is split between both the state and federal governments. While this is the ideal scenario, it must be understood that only 62 percent of utilities are publically owned in the first place. Also notable is the fact that investor-owned utilities serve 68 percent of people, meaning the burden on publically owned utilities is smaller.[334]

The transition to having numerous microgrids would have to begin with the publically owned utilities, as the investor-owned utilities do not have any motivation to spend the extra initial money. Since the publically owned utilities are going to be the ones to initially make the transition, critical infrastructures will continue to receive priority over residential or commercial areas As demonstrated through the UCSD microgrid, a grid the size of a tennis court can accommodate a very large number of people. This makes it practical in a large city, as many people live and operate in a smaller area.

Microgrids are an extremely useful tool, and serve as an insurance policy for the grid. The primary two benefits are the island effect and the ability to use renewable energy sources. In a time when moving away from petroleum based energy is prioritized, microgrids can provide a relatively small-scale solution with potential for expansion. The success of small-scale projects shows promise for future projects, and the obstacles can be overcome. The concerns regarding cost are legitimate, but the long-

[334] The White House. "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages.". https://www.smartgrid.gov/document/economic_benefits_increasing_electric_grid_resilience_weather_outages (accessed January 1, 2014).

term benefits can outweigh the expense of the initial investment. UCSD reports savings of $800,000 per month solely due to the microgrid—the system clearly pays for itself. [335] Although funding microgrids is not a popular political move currently, efforts to improve the grid could have significant positive effects in both the short-term and long-term.

## MICROGRID RAMIFICATIONS

While the gains in efficiency, reliability, and cost-effectiveness appear attractive, there are unresolved concerns about the security of microgrids and the long-term impact on the broader bulk power system.

The larger bulk power system will continue to be needed for load balancing and to provide power to microgrids that may experience disruptions in generating capacity. Such situations may occur when solar panels do not receive enough sunlight, or wind farms faced becalmed weather. However, in an electricity market made up solely of microgrids, there would be little in the way of continued economic incentives for the transmission infrastructure and central generation needed to provide bulk power. As a result, such back up systems could potentially require significant support through methods that many consider market distorting—such as direct subsidies or tax credits.

Furthermore, in an environment where the central utility business model would be slowly dismantled, there would be difficulties in ensuring the support of major investor owned utilities in providing the continued investment in security and infrastructure improvements.

In terms of security, while the microgrids would theoretically provide increased redundancies, there would be a need to secure a significantly greater number of additional sites, facilities, and systems. Further examination of the workforce requirements and security needs of a widely implemented microgrid system is necessary.

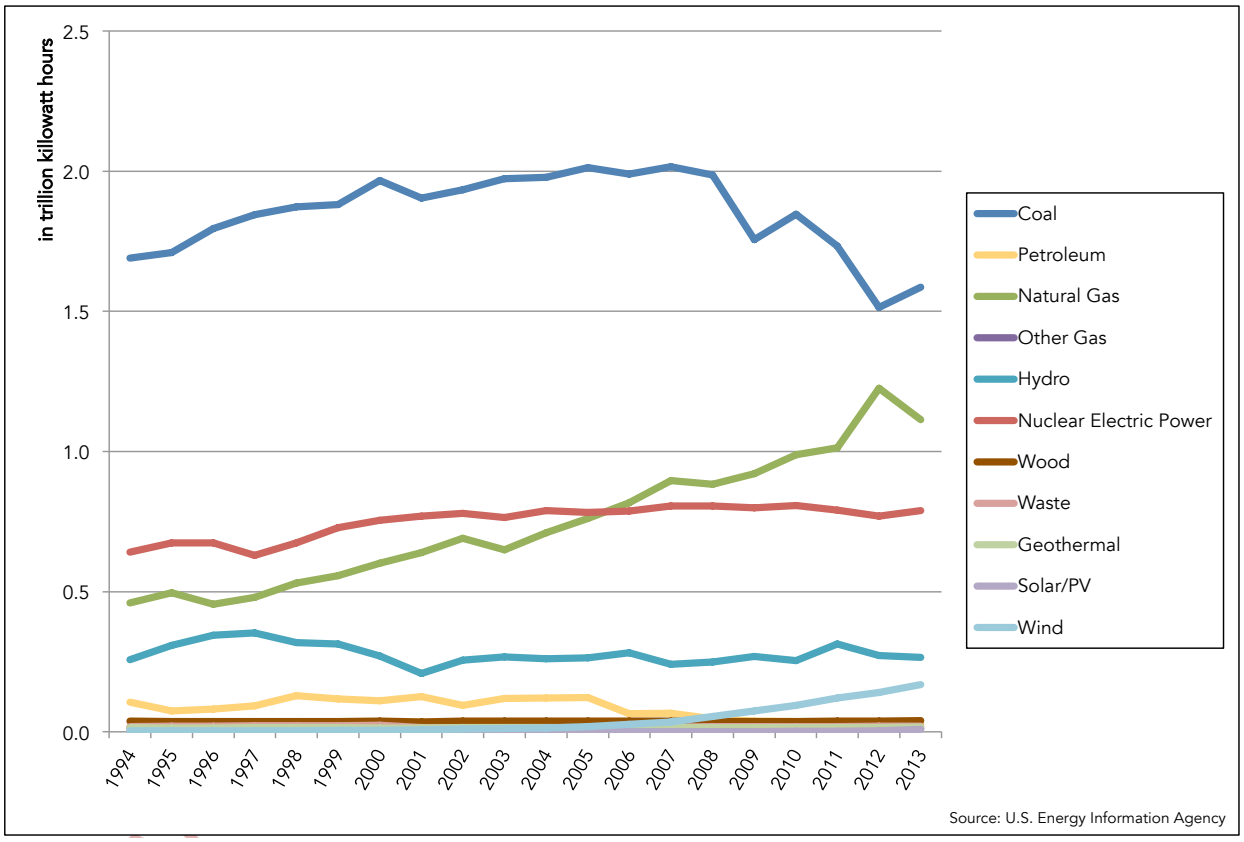
[335] EcoMotion. "The U.C. San Diego Microgrid." . http://ecomotion.us/2013/01/the-u-c-san-diego-microgrid/ (accessed January 1, 2014).

## FUTURE OF GENERATION SOURCES

One of the major future transitions for the electrical grid is the changing dynamics in generation sources. The future reliability and security of the grid will also depend on how policy makers address the nation's changing energy portfolio and the need to responsibly reduce carbon emissions. As the breakdown of electricity supply by generation source illustrates, coal remains the preeminent fuel source even with advances in natural gas generation. Even with increased investments in sources such as wind and solar, nuclear power remains the most significant source of carbon-free generation.

Changes in the nation's generation portfolio will require major investments in both electrical infrastructure, as well as ancillary systems. While this is by no means a comprehensive analysis of these challenges, this report seeks to raise these issues for policymakers and analyze the lessons from where some of these shifts in generation have already taken place—notably Germany.

**TRENDS IN GENERATION & RENEWABLES**



## THE NATURAL GAS BOOM & THE FUTURE OF COAL

Natural gas is a hydrocarbon gas mixture mostly comprised of methane, a nonrenewable fossil fuel found within porous rock formations or shale basins. Similar to other fossil fuels, natural gas is a primary energy source and is the second largest source after petroleum. With the recent development of new technology and the current Administration's policies aimed at curbing coal use, natural gas has become more economically and politically popular. Despite the natural gas boom and the regulatory hurdles looming for coal power, major infrastructure challenges remain.

The majority of the natural gas resources are found in traditional gas formations within the Middle East—Iran, Qatar, and Saudi Arabia—followed by significant resources in the United States and Russia. The United States has grown in prominence as technologies such as hydraulic fracturing—or "fracking"—have allowed for the recovery of natural gas from shale formations.

Due to the success in recovering natural gas from these shale formations, companies have begun to take advantage of the abundant natural resources throughout the country. Over the past decade, multiple shale plays have been discovered and utilized within the continental United States. The largest shale plays are Bakken Shale (North Dakota and Montana), Barnett (Texas), Woodford (Oklahoma), Eagle Ford (Texas), Niobrara (Wyoming, Nebraska, Colorado, and South Dakota), Marcellus (Adirondacks), Haynesville (Arkansas, Louisiana, and Texas), and Permian (Texas).[336] Over the past years, the production of natural gas had continued to increase to 24 trillion cubic feet and provides the country with about 25 percent of its overall energy needs.

Due to the abundant resources within the United States, many have advocated that natural gas-powered electricity generation is the most reliable option. Unlike solar or wind, natural gas can act as base load power generation because it does not fluctuate or depend upon weather patterns.[337] Currently, the vast majority of natural gas power plants are used as supplemental stations, taking advantage of natural gas's quick firing characteristics to provide additional generation.

Additionally, substantial infrastructure changes must be made to successfully integrate natural gas into the electrical grid on a scale that could provide base load capacity and replace coal as a main generation source. Of particular note, natural gas power plants

---

[336] Ana Komnenic, "Here's how the US is becoming the world's biggest oil and gas producer," *Mining.com,* November 18, 2013, http://www.mining.com/heres-why-the-us-is-about-to-become-the-worlds-biggest-oil-and-gas-producer-69714/

[337] David Blackmon, "Natural Gas: The Electrical Grid's 20 Minute Pizza," *Forbes,* January 17, 2014, http://www.forbes.com/sites/davidblackmon/2014/01/17/natural-gas-the-electric-grids-20-minute-pizza/

lack coal power plants' ability to store fuel onsite, requiring the installation of new pipelines to the plant or the development of compressed or liquefied natural gas storage. [338] Due to regulatory restraints, high construction costs, and local opposition, both utilities and gas suppliers currently have limited options in addressing these infrastructure challenges. Ultimately, multiple sectors must adapt in order for natural gas to fully reach its potential as a resource for generation.

In terms of coal-burning generation, there are significant regulatory and technical hurdles looming in the near future. The Obama Administration and Environmental Protection Agency (EPA) have begun an active campaign to reduce fossil fuel emission levels. In June of 2014, the EPA proposed standards for coal-fired power plant, which would result in a 30 percent reduction of emission levels by 2030.[339] As electrical utilities are focusing their attention on developing renewable energy sources, coal continues to play a major role in electricity generation. As of 2013, the country generated approximately 4,058 billion kilowatt hours of electricity and 39 percent of the electricity generated came from coal.[340]

The backbone of the electrical grid comes from base load generation or the minimum level of electrical demand over a 24-hour period. Typically, both coal and nuclear have predominately acted as base load generation considering that they operate at a full, steady output. This is unlike other sources of energy generation such as wind or solar, which are affected by weather patterns or natural gas plants that are quickly stopped or started depending on varying demand. In addition, electrical generation within the country has varied by region depending upon resources and cost. Furthermore, while some states, such as California have transitioned away from coal generation, other states—such as Kentucky and Indiana—rely on coal for over 85 percent of electricity generation.[341]

As a result, it would be impossible to fully eliminate coal as a source of energy generation within this country. Increases in efficiency and the shutting of the most heavily polluting plants could meet both some of the regulatory standards and off-peak

---

[338] Vicki Ekstrom, "Grid Reliability and the Role of Natural Gas," *MIT Energy Initiative,* May 6, 2014, http://mitei.mit.edu/news/grid-reliability-and-role-natural-gas

[339] John H. Cushman Jr., "How Ambirious is EPA's Climate Change Rule, Really?" *InsideClimate News,* June 3, 2014, http://insideclimatenews.org/carbon-copy/20140603/how-ambitious-epas-climate-change-rule-really

[340] "What is U.S. electricity generation by energy source?" *U.S. Energy Information Administration,* June 13, 2014, http://www.eia.gov/tools/faqs/faq.cfm?id=427&t=3

[341] Dawn Santoianni, "The Backbone of the Electric System: A Legacy of Coal and the Challenge of Renewables," *Scientific American,* May 17, 2012, http://blogs.scientificamerican.com/guest-blog/2012/05/17/the-backbone-of-the-electric-system-a-legacy-of-coal-and-the-challenge-of-renewables/

base load needs, but coal will continue to be a part of the U.S. generation portfolio for the foreseeable future.

If the United States were to greatly reduce its coal generation, consumers would face significant increases in energy costs, and, in all likelihood, the coal not used in the United States would be exported overseas—thus negating any carbon reduction goals.

A solution for these challenges is continued investment in carbon-capture-and-sequestration (CCS) technology that allows for continued coal generation that meets environmental goals. Using CCS technology, carbon dioxide emitted from power plants is injected into rock formations deep underground, thus trapping the carbon dioxide and preventing it from entering the atmosphere. While this technology is expensive and outstanding questions about its effectiveness remain, development and installation of CCS technology could allow existing coal power plants to continue to provide their significant portion of electric generation.

## THE VITAL ROLE OF NUCLEAR

Within the United States, 100 nuclear power reactors are spread across 31 states, which account for 20 percent of the electricity generated and for 64 percent of the zero-carbon emission generation sources (nuclear, hydro, solar, wind, etc.).[342]

The high and wide range of costs associated with power plants have deterred many from supporting nuclear power. Not only does it take approximately 10-15 years to build a nuclear power plant, but to properly maintain the plant, owners must factor in capital costs (construction and financing); plant operating costs (fissile material and decommissioning); system costs; and external costs. For example, the cost to obtain 1 kg of uranium as reactor fuel is estimated at $1,160 USD, yet that amount of uranium will produce about 20,000 times as much energy as the same amount of coal.[343] Additionally, nuclear generation—in terms of both construction and operation costs—currently finds it difficult to compete against relatively inexpensive natural gas systems.

Many critics of nuclear power believe that there are high risks associated with this form of energy and cite the disaster at the Fukushima Daiichi power plant in 2011 as an example. Even though there are extensive international and national regulations

[342] "Nuclear Power in the USA," *World Nuclear Association*, February 20, 2014, http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/USA--Nuclear-Power/

[343] "The Economics of Nuclear Power," *World Nuclear Association*, February 2014, http://www.world-nuclear.org/info/Economic-Aspects/Economics-of-Nuclear-Power/

concerning the construction and maintenance of nuclear power plants, the combination of a tsunami and Tohōku earthquake critically damaged the plant. Contaminated water and radiation have been two of the results associated with the meltdown of three of the plant's six nuclear reactors.[344]

As controversy surrounding the reliability of nuclear power plants continues and reliance upon other forms of renewable energy increases, California and Germany can be examined as useful case studies. California has been undergoing a "renewable revolution," in which the state is currently shifting towards renewable fuels and away from nuclear energy due to its environmental impact, safety concerns, and maintenance costs. Previously, California had five operational nuclear power plants, but as of 2012, only one was in operation. Currently, the Diablo Canyon power plant, owned by PG&E, is the only plant operating within the state. This plant is located near San Luis Obispo and has two Units—operational in 1985 and 1986.[345]

Additionally, there was fundamental policy shift within Germany beginning in 2011 after the Fukushima nuclear power plant disaster. After Chancellor Angela Merkel's administration came under immense pressure to secure energy sources within the country, the government initiated the *Energiewende* policy. This energy policy is focused on developing solar and wind capabilities, while decreasing the country's reliance upon nuclear energy.

During March of 2011, the autonomous Reactor Safety Commission (RSK) assessed the safety and security of the 17 nuclear power plants spread throughout the country. The RSK published their findings, stating that German plants were secured through the implementation of safeguards. Yet, the Merkel administration decided that the cost of a nuclear disaster was too great and decided to phase out nuclear energy over the next decade.[346] "Chancellor Angela Markel decreed that the country's nuclear power reactors which began operation in 1980 or earlier should be immediately shut down. Those units then closed and were joined by another unit already in long-term shutdown, making a total of 8,336 MWe offline under government direction, about 6.4

---

[344] Hiroko Tabuchi, "Reversing Course, Japan Makes Push to Restart Dormant Nuclear Plant," *The New York Times,* February 25, 2014, http://www.nytimes.com/2014/02/26/world/asia/japan-pushes-to-revive-moribund-nuclear-energy-sector.html?_r=1

[345] "Nuclear Energy in California," *California Energy Commission,* 2014, http://www.energy.ca.gov/nuclear/california.html

[346] "Developments in Germany following the nuclear disaster in Japan," *Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety,* March 10, 2014, http://www.bmub.bund.de/en/topics/nuclear-safety-radiological-protection/nuclear-safety/response-to-fukushima/overview/

percent of the country's generating capacity."[347] By the end of 2022, the German government plans to close the nine remaining nuclear power plants.

In response to concerns about cost and safety, many companies have begun to reexamine nuclear power plant technology in an attempt to cut costs and increase resilience. For example, the Babcock & Wilcox Company is developing a series of small modular reactors (SMR) called the B&W mPower reactor. A SMR is a new generation nuclear power plant, which has an output of less than 500 MWe and a natural cooling feature. Not only do they increase the security of fissile material, they are designed to be more cost effective and environmentally acceptable than traditional power plants.[348]

Other potential innovations include developments in thorium reactors or pebble-bed reactors that provide increased reliability and self-limiting reactions that largely negate meltdown or radiation emission concerns.

If a major developed economy like the United States is going to meet its future energy needs while reducing carbon emissions, nuclear power must be one of the generation sources supported by policy makers. While it has its own significant challenges in terms of cost, politics, and infrastructure, it represents one of the better paths forward for providing long-term base load that complements the fluctuations in renewable generation.

## THE GROWTH OF RENEWABLES

Improving our electrical grid infrastructure is interrelated with developing a resilient approach to energy consumption. Updated grid infrastructure can increase the efficiency of energy use, while also allowing the United States to harness the natural resources available through the shale oil and gas revolutions, as well as the implementation of renewable energy sources through distributed energy resources (DER).

On a national level, the Obama Administration has been promoting its "All of the Above" strategy, which focuses on energy resilience and independence. This policy focuses upon a shift away from coal to natural gas; increasing the nations reliance upon alternative energy sources (solar, hydro, and wind); and decreasing energy costs.

---

[347] "Nuclear Power in Germany," *World Nuclear Association,* July 2014, http://www.world-nuclear.org/info/country-profiles/countries-g-n/germany/

[348] "B&W mPower Reactor," *The Babcock and Wilcox Company,* 2014, http://www.babcock.com/products/Pages/mPower-Reactor.aspx

Especially with the development of new technology and methodologies, such as fracking, the adherence to this policy has become more realistic.

In addition to the national policy, many states have begun to implement their own energy policies, which focus upon lowering carbon emissions and integrating renewables into the electrical grid. For example, in 2011, California passed a law mandating the state to obtain 33 percent of its power from renewables by 2020. AB 327 specifically removes many of the restrictions on developing forms of distributed energy resources, such as solar panels, and alters the electricity rate structures and process of selling electricity back into the grid. Net metering "allows utilities to flatten the higher prices per kilowatt-hour that heavy residential power users pay for marginal amounts of electricity used on a month-by-month basis, and provide the potential for them to charge flat monthly fees to all residential customers."[349] Utilities have argued that net metering does not adequately compensate for the costs they face in supplying solar photovoltaic technology. As a result, they have been forced to raise rates to non-solar customers or are faced with negative revenue.

One of the major difficulties with implementing renewables is the fluctuation in generation capacity. The variations in wind and solar can result in energy surpluses or shortfalls, and technology for providing reliable storage remains on the drawing board—especially in a distributed generation system. Current technologies, such as hydro storage—where excess electricity is used to fill a reservoir that later provides hydropower when additional generation is needed—are designed largely around the centralized grid model and its long-distance transmission infrastructure. Advances in localized storage will address these challenges, but the U.S. electrical grid will still require a business model that supports some level of centralized infrastructure and base load generation.

Additionally as components of Smart Grid are being integrated into renewable energy infrastructure, equipment such as wind turbines becomes vulnerable to cyberattacks. Recently, a cross-site scripting (XSS) flaw in the control portal (NC2) manufactured by Nortex was discovered, which is a SCADA/HMI product. The Nortex NC2 software application gives users a portal to control the wind turbines that they manage, so they may receive data and reports. This vulnerability is remotely exploitable and could give an attacker the ability to run code on a compromised machine.[350] As threat actors

---

[349] Jeff St. John, "AB 327: From California Solar Killer to Net Metering Savior?" *Greentech Media*, September 3, 2013, http://www.greentechmedia.com/articles/read/ab-327-from-california-solar-killer-to-net-metering-savior

[350] Dennis Fisher, "ICS-CERT Warns of Flaw in Wind Farm Management App," *Threat Post*, December 17, 2013, http://threatpost.com/ics-cert-warns-of-flaw-in-wind-farm-management-app

continue to develop their capabilities, it is imperative that utilities implement security protocols to secure distributed generation equipment from cyberattacks.

### *Lessons from Germany*

The German *Energiewende*—"energy turn"—is one of the most comprehensive shifts towards renewable electricity taken by any nation. The basis of this energy policy is to shift away from the country's reliance upon nuclear power and towards renewable sources of generation, such as wind, biomass, hydropower, and photovoltaic. The Merkel administration has stated that it "would stick to the objective of reducing greenhouse gas emissions by 40 percent by 2020 (compared with 1990 levels) and by 80 percent by 2050."[351]

Three years after this national policy went into effect, the country is confronted with rising energy costs, inefficient grid architecture, and an increased dependence on coal energy. Even with the integration of 1.4 million solar photovoltaic installations and 24,000 wind turbines throughout the country, nuclear power still accounted for 75 percent of power generation in 2013.[352]

Additionally, without grid architecture and storage solutions designed for the fluctuations in the production of renewable energy—e.g. changes in wind speed or sunshine—German utilities have found themselves dealing with major fluctuations in the electricity supply. In order to provide more stability in input costs, major German manufacturers have both lobbied for reduced or subsidized electricity contracts and installed onsite generation or cogeneration facilities. During summer months, German utilities have been confronted with negative wholesale electricity prices—reflecting a glut of electricity in the grid. At other times, as renewables have not met electricity demands, German utilities have turned to the use of coal power plants. Thus, almost three years into the *Energiewende,* Germany has electricity rates 50 percent higher than the rest of Europe, and it has seen growth in its carbon emissions over the past two years.[353]

---

[351] Hardy Graupner "What exactly is Germany's 'Energiewende'?" *Deutsche Welle,* January 22, 2013, http://www.dw.de/what-exactly-is-germanys-energiewende/a-16540762

[352] Jeffrey Michel, "Can Germany survive the Energiewende?" *RenewEconomy,* March 31, 2014, http://reneweconomy.com.au/2014/can-germany-survive-energiewende-33428

[353] "German Energy Prices 50% Higher than EU Average: McKinsey," Text, *EurActiv - EU News & Policy Debates*, February 7, 2014, http://www.euractiv.com/sections/energy/german-energy-prices-50-higher-eu-average-mckinsey-269844; "Energiewende-Deutschlands CO2-Emissionen Steigen Weiter an," *Die Zeit*, April 8, 2014, sec. wirtschaft, http://www.zeit.de/wirtschaft/2014-04/grafik-co2-emissionen.

# CSPC BOARD OF TRUSTEES

**THE HONORABLE DAVID M. ABSHIRE**
*Vice Chairman of the Board*
Center for the Study of the Presidency & Congress

**MAXMILLIAN ANGERHOLZER III**
*President & CEO*
Center for the Study of the Presidency & Congress

**ANDREW F. BARTH**
*President*
Capital Guardian Trust Company

**THE HONORABLE WAYNE L. BERMAN**
*Senior Advisor*
The Blackstone Group

**MAURY BRADSHER**
*Chairman & CEO*
District Equity

**ELI BROAD**
*Founder*
The Broad Foundation

**THE HONORABLE R. NICHOLAS BURNS**
*Professor of the Practice of Diplomacy and International Politics*
John F. Kennedy School of Government
Harvard University

**JAY COLLINS**
*Vice Chairman*
*Corporate and Investment Banking*
Citi

**ROBERT A. DAY**
*Chairman & CEO*
Oakmont Corporation

**BRADFORD M. FREEMAN**
*Founding Partner*
Freeman Spogli & Co.

**THE HONORABLE DAVID GERGEN**
*Professor*
John F. Kennedy School of Government Harvard University

**DR. MALIK M. HASAN**
*Founder*
Health Net, Inc. & Health Trio, Inc.

**THE HONORABLE STUART W. HOLLIDAY**
*President & CEO*
Meridian International Center

**DR. RAY IRANI**
*Chairman & CEO*
Ray Investments, LLC

**DANIEL C. LUBIN**
*Founder & Managing Partner*
Radius Ventures

**THE HONORABLE MEL MARTINEZ**
*Chairman of the Southeast United States & Latin America*
JPMorgan Chase & Co.

**THE HONORABLE THOMAS F. MCLARTY III**
*President*
McLarty Associates

**THE HONORABLE EDWIN MEESE III**
*Ronald Reagan Distinguished Fellow*
The Heritage Foundation

**THE HONORABLE GLENN C. NYE III**
*Senior Advisor*
Palantir Technologies

**THE HONORABLE GERALD L. PARSKY**
*Chairman*
Aurora Capital Group

**THE HONORABLE THOMAS R. PICKERING**
*CSPC Chairman of the Board*
*Vice Chair*
Hills & Company

**H. GREGORY PLATTS**
*Former Senior Vice President & Treasurer*
National Geographic Society

**THE HONORABLE THOMAS J. RIDGE**
*President*
Ridge Global, LLC

**THE HONORABLE FRANCIS ROONEY**
*CEO*
Rooney Holdings, Inc.

**B. FRANCIS SAUL III**
*Chairman & CEO*
Saul Investment Group, LLC

**PAMELA SCHOLL**
*CSPC Vice Chairman of the Board*
*CSPC Chairman of the Executive Committee*
*Chairman & President*
The Dr. Scholl Foundation

**STEPHEN A. SCHWARZMAN**
*Chairman, CEO, & Cofounder*
The Blackstone Group

**THE HONORABLE RICHARD H. SOLOMON**
*Senior Fellow*
RAND Corporation

**GEORGE STEPHANOPOULOS**
*Chief Anchor*
ABC News

**THE HONORABLE ROBERT H. TUTTLE**
*Co-Managing Partner*
Tuttle-Click Automotive Group

**THE HONORABLE TOGO D. WEST JR.**
*Chairman*
LTI Leadership Group

**STANLEY R. ZAX**
*Former Chairman, President, & CEO*
Zenith National Insurance Corporation


CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

1020 19th Street, NW Suite 250 | Washington, DC 20036 | 202-872-9800 | www.thePresidency.org