# Protecting America's Electric Grid Against Cyberattack

**March 2017**

Foundation for Resilient Societies
52 Technology Way
Nashua NH 03060
www.resilientsocieties.org

## Executive Summary

Cyberwarfare against electric grid control and communications systems is a growing threat to national security. In 2014, Russian computer malware widely infected electric power plants in the Western Europe and the United States, causing the director of the National Security Agency to confess before Congress that nation-states could take out America's grid. In December 2015, and again in December 2016, cyberattacks blacked out electric customers in Ukraine. The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on control systems for critical infrastructure. Laptop computers and internet connections can be better than bombs for attacking electric grids. A cyberattack on America's electric grid is an existential threat, because an effectively planned and executed attack could cause a nationwide blackout lasting for months or years.

Powerful economic incentives have exacerbated electric grid cyber-vulnerabilities. In search of operational efficiencies and cost savings, utilities and their vendors have made direct and indirect connections of electric grid communication and control equipment to the public internet. Despite security briefings by the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS), utility managers continue to increase internet connectivity, year after year. The internet provides cheap interconnections, but also provides wide avenues for attack by foreign powers, terrorist groups, and individual hackers.

During build-out of America's electric grid, its control systems were intentionally designed without integrated cybersecurity, because it was not anticipated that these systems would someday be connected to the public internet. Instead, utilities assumed that restricting physical access would be adequate protection.

When electric grid equipment is connected to the internet, it can be more easily monitored and remotely reconfigured. Internet communications for utilities can be cheaper than dedicated data links. The internet-enabled "Smart Grid" delivers lower cost electricity and allows more responsive conservation by consumers. In a recent development, even software applications for grid control are being placed in the internet "cloud."

Stronger grid cybersecurity will require utilities to work internally and with equipment vendors to correct the most severe vulnerabilities. Cybersecurity must be integrated into foundry chipsets, components, and equipment designs; and firmware must come from trusted sources, because malware embedded in original firmware may be undetectable by ultimate customers. Because the average lifetime of installed equipment is several decades, insecure legacy equipment must be identified and replaced. Utilities have no easy cost recovery mechanisms for more rapid cybersecurity improvements. Inability to recover costs causes utilities to resist mandatory cybersecurity standards.

As a cheap stopgap measure, utilities have installed "firewalls." Firewalls often have security flaws. As an alternative solution, some cybersecurity experts have proposed "air-gapping"—

completion isolation of utility control systems from the public internet. However, improved management of electric grid operations requires continuous communication between business systems and grid control systems, making air-gapping difficult and economically disadvantageous.

Societal pathways to better cybersecurity protection include legislation, executive orders, mandatory standards, industry standards, voluntary measures, and establishment of financial liability for utilities. During the coming decade or more while protections are improved, cyber-deterrence against foreign adversaries will be essential.[1]

In the near term, the outlook for cybersecurity protection of the U.S. electric grid is fair to poor. Operational efficiencies and cost-saving measures drive cybersecurity vulnerabilities. The electric utility industry lacks funding for protective measures. Economic incentives are prevailing over costly cybersecurity retrofitting.

## Cyberattack Threat

The opportunity for operational efficiencies, as well as pressure for cost savings, have caused America's electric utilities to intertwine their computer systems with the public internet. The public internet is increasingly used for cheap communication among electric grid control rooms, transmission and distribution substations, and generation facilities; these communications are often unencrypted and therefore vulnerable to interception and modification. The Smart Grid requires constant communication among grid control systems and metering/switching devices at customer locations—for example, when electricity supply is constrained, electric hot water heaters in homes may be turned off. The internet is a quick and cheap way to establish Smart Grid communications.

### Architecture Basics: Operational Technology and Information Technology

The architecture of computer systems used in electric utilities can be divided into two basic segments. Operational Technology used for direct control of electric grid operations—bringing generation plants on and offline, configuring transmission pathways, and distributing of power to homes and businesses. Information Technology (also commonly called "business systems")—handles utility functions such as accounting, billing, and customer service. The desktop computers of most utility employees would also fall into the category of Information Technology.

As with other industries, employees of electric utilities commonly use software applications that depend on the public internet—examples include email and web browsing. Most computer users intuitively understand that Information Technology such as email must be connected to the public internet, even indirectly.

[1] See James N. Miller, James R. Gosler, et al., *Task Force on Cyber Deterrence*, Report. February 2017. Accessed March 31, 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

At electric utilities, Operational Technology is increasingly connected to the public internet, albeit indirectly through Information Technology. Improved automation at electric utilities requires deliberate connection between Operational Technology and Information Technology. For example, measures of electricity flow collected by Operational Technology may be used for accurate bill preparation by Information Technology—this data exchange requires electronic linkages, which have the side effect of establishing indirect connections to the public internet.

## Internet Connections Cause Cybersecurity Vulnerabilities

Importantly, Operational Technology used for grid control was originally designed to be protected only by restriction of physical access and therefore commonly lacks integrated security. A good analogy might be single-family homes protected by front door locks, but without locked doors between the kitchen, dining, and living rooms, so that the residents and trusted guests can communicate and freely move about.

In modern times, thieves need not defeat front door locks to rob homeowners; instead, they can use internet connections to steal bank account numbers and passwords from personal computers. Likewise, intruders need not break down the doors of utility control rooms to take over electric grids; instead, they can exploit direct and indirect connections to the public internet.[2]

## Firewalls as a Partial Solution

Recognizing the threat of cyberattack through the public internet, utilities have attempted to establish protection for their Information Technology and Operational Technology with computerized barriers — so-called "firewalls." (The term "firewall" was originally used to indicate a barrier for another security threat—the spread of fire within businesses and residences.) Firewalls have become a well-accepted security solution.

Nonetheless, firewall protection is incomplete and imperfect. Firewalls commonly used in electric grids have been found to contain security flaws such as "hard-coded passwords" and "backdoors."[3] Moreover, firewalls can have coding flaws that allow attackers to break through.[4] Just as physical firewalls will not prevent the spread of all fires, computer firewalls will not halt all cyberattacks.

---

[2] For an extensive discussion of how interconnections between Information Technology and Operational Technology networks can cause cyberattack vulnerability for control systems, see ICS-CERT Alert (IR-ALERT-H-16-056-01), "Cyber-Attack Against Ukrainian Critical Infrastructure," February 25, 2016. Accessed March 30, 2017. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 .

[3] See Juniper Networks, "Important Announcement about ScreenOS," December 17, 2015. Accessed March 30, 2017. https://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554.

[4] See Cisco, "Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability," February 10, 2016. Accessed March 30, 2017. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike.

## Malware Threat

Security shortfalls in firewalls and otherwise can allow attackers to install "malware" into both Operational Technology and Information Technology. Malware typically establishes communication channels (command and control) through the public internet back to the cyber-attackers. Even without continual communication, advanced malware can act semi-autonomously to disrupt grid operations. Malware can be designed to steal user credentials, including passwords; at a time of attackers choosing, stolen user credentials can be used to take complete control of both Operational Technology and Information Technology.

## Disruption of Electric Grid Control

At any point in time, the production of electricity by utilities must exactly balance with its consumption. Cyber-attackers seek to disrupt finely tuned electric grid control that is vital for grid stability. Attackers can take over control of electricity production, consumption, or both. For example, cyberattacks can shut off generation facilities. Alternatively, commands to open breakers at substations can interrupt the flow of electricity to homes and businesses. Grid control may be disrupted at the highest level — within control centers — or at lower levels such as substations.

When customer demand for electricity does not balance with generated supply, a cascading grid collapse can result. During a cascading collapse, excess power can harmfully surge into grid equipment. Power surges cause over-voltages that can catastrophically damage breakers, generators, transformers and customer equipment. Delays in replacing grid equipment can prevent power restoration or necessitate long-term rolling blackouts when the network is restored. Typical replacement lead times for generators and high-voltage transformers are in excess of one year. The substantial majority of large power transformers are manufactured outside of the United States.

Some larger and more capable utilities have installed multiple layers of defense to protect against cyberattack. However, because all utilities are electrically interconnected, and because a simultaneous attack on smaller utilities can cause a cascading collapse for the entire grid, the grid remains vulnerable.

## Interruption of Essential Services

Attackers may also interrupt essential services for electric grid facilities, apart from direct operational control. For example, attackers can turn off electric power for control rooms, communication facilities, and substations. Turning off heating ventilation and air-conditioning systems (HVAC), or water cooling and recycling systems, can also disrupt electric grid operations.

Attacks unrelated to the flow of electricity can nonetheless cause significant disruption to reliable electric service. For example, if customer service centers are flooded with automated phone calls, then legitimate phone calls from blacked-out customers can be blocked — a so-

called "Telephony Denial of Service" (TDoS) attack. The grid remains vulnerable to a wide range of Distributed Denial of Service (DDoS) attacks.

### Grid Restoration Challenges

When a widespread electric grid outage occurs, utilities are in a race against time to restore power. Backup power for electric grid facilities has limited duration. For example, substation battery power typically lasts eight hours. Diesel fuel for backup generators at control rooms is also limited, with typical reserves of just a few days. Utilities commonly have pre-established contracts for resupply of diesel fuel, but during a wide-area power outage, delivery may not be assured.

After a cyberattack, utilities will likely be forced to dispatch technicians to substations to manually close circuit breakers and switches, time-consuming steps requiring close communication to avoid equipment damage and shock hazards to line workers. When the electric grid is partially restored, it may collapse again because of difficulty matching electricity production with demand. Each grid restoration attempt takes more time and expends more emergency fuel. When backup generator fuel for control centers and communications is exhausted, grid restoration will become far more challenging.

## Wake-Up Calls: Grid Cyberattacks

Increasingly, nations view critical infrastructure as a battlefield of the future. Foreign nations are using cyberattacks for reconnaissance, electric grid debilitation, and diplomatic signaling.

### BlackEnergy Incursions

In 2014, Russia conducted widespread cyber-incursions into U.S. electric utilities. Emails were the means of cyberattack, with attachments containing Russian "BlackEnergy" malware hidden in Microsoft Office files. No wide-area blackouts resulted. However, in November of 2014, Admiral Michael Rogers, Director of the National Security Agency and Commander of U.S. Cyber Command, testified to Congress that Russia, China, and other nations could take down the U.S. electric grid at a time of their choosing.[5]

### Ukraine Grid Cyberattack

On December 23, 2015, a cyberattack in Ukraine caused a blackout for 225,000 people. Russian attackers first placed malware within the Information Technology of distribution utilities using BlackEnergy "droppers" in email messages. This malware was used to steal user credentials. Attackers then used stolen credentials to pivot into the Operational Technology of the utilities, where they took control of energy management systems. Through internet access to operator

[5] Testimony of Admiral Michael S. Rogers, Director, National Security Agency, and Commander, U.S. Cyber Command, "Cybersecurity Threats: The Way Forward," before the U.S. House Permanent Select Committee on Intelligence. November 20, 2014. Accessed March 30, 2017. https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml.

consoles, the attackers remotely opened switches in 30 substations, shutting off power to about 225,000 electricity consumers.

In a clever second punch, the attackers used internet access to schedule shutdowns for the Uninterruptible Power Supplies (UPS) at grid substations. The attackers also overwrote firmware in critical substation equipment to prevent quick restoration of power. Because of cyberattack-caused loss of remote control, restoration of electricity required utilities to dispatch technicians to grid substations to manually close circuit breakers.

Coincident with the December 2015 blackout, customer service centers in Ukraine were flooded with bogus telephone calls, preventing electricity consumers from reporting outages. Lack of outage information at utilities further delayed power restoration.[6]

In December 2016, the Ukraine grid was hit with another cyberattack, this time on the Kiev transmission system; and also on the state pension system, railroad system controls, mining corporations, and the Kiev airport. The persistence of cyber-vulnerabilities, even after a first-round attack, was made abundantly clear.[7]

## The Stakes for America

Contemporary American society depends on continuous electric power. An effectively executed cyberattack could cause loss of electricity over large geographic areas for months or years. Without power, water supply and sanitation systems will stop operating. Food refrigeration and distribution will cease. Police and fire stations will lack power to continue operations; civil disorder will result. Gas station fuel pumps and traffic control will be interrupted, impeding evacuation of major metropolitan areas.

Even a geographically-limited cyberattack on the U.S. electric grid could cause crippling financial losses for the American economy. In 2015, Lloyd's published a cost estimate of damages resulting from a cyberattack on the U.S. power grid.[8] The Executive Summary reads in part:

> Business Blackout, a joint report by Lloyd's and the University of Cambridge's Centre for Risk Studies, considers the insurance implications of a cyber attack on the US power grid.

---

[6] See SANS Institute and Electricity Information Sharing and Analysis Center (E-ISAC), *The Analysis of the Cyber Attack on the Ukrainian Power Grid; Defense Use Case 5*. Joint Report. March 18, 2016. Accessed March 30, 2017. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf .

[7] See Smith, R., "Fears Over U.S. Power Grid; Recent cyberattacks in Ukraine raise alarms over vulnerability of infrastructure here," *Wall St. Journal,* December 31, 2016. and *BBC News*, "Ukraine power cut 'was cyber-attack," January 11, 2017. Accessed March 31, 2017. http://www.bbc.com/news/technology-38573074.

[8] *Business Blackout; The insurance implications of a cyber attack on the US power grid*. Report. Cambridge Centre for Risk Studies, University of Cambridge. May 2012. Accessed March 27, 2017. https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

> This report publishes, for the first time, the impacts of this sort of attack using the hypothetical scenario of an electricity blackout that plunges 15 US states including New York City and Washington DC into darkness and leaves 93 million people without power. The scenario, while improbable, is technologically possible and is assessed to be within the benchmark return period of 1:200 against which insurers must be resilient.
>
> In the scenario, a piece of malware (the 'Erebos' trojan) infects electricity generation control rooms in parts of the Northeastern United States. The malware goes undetected until it is triggered on a particular day when it releases its payload which tries to take control of generators with specific vulnerabilities. In this scenario it finds 50 generators that it can control, and forces them to overload and burn out, in some cases causing additional fires and explosions. This temporarily destabilises the Northeastern United States regional grid and causes some sustained outages. While power is restored to some areas within 24 hours, other parts of the region remain without electricity for a number of weeks.
>
> Economic impacts include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain. The total impact to the US economy is estimated at $243bn, rising to more than $1trn in the most extreme version of the scenario.

Long-term loss of electric power can have catastrophic second-order effects on other critical infrastructures. For example, when spent fuel pools at nuclear power plants lack electric power for cooling, the water can boil off and expose hot fuel rods to the open air. The rods can then catch fire, releasing a plume of deadly radiation. During the 2011 Fukushima disaster in Japan, emergency managers feared that one of the nuclear plant spent fuel pools had gone dry, nearly causing an order for the evacuation of Tokyo. Approximately 100 nuclear power plants in the United States have spent fuel pools that could catch fire during long-term loss of grid power.

As another example of second-order effects, earthen dams in the western U.S. have electrically actuated gates for water control. Loss of dam control could cause overtopping and erosion of spillways, resulting in dam failure and catastrophic flooding of downstream population centers.

All life-supporting critical infrastructures ultimately depend on electric power. According to 2008 congressional testimony of Dr. William Graham, former Presidential science advisor, casualties in the aftermath of a nationwide infrastructure outage lasting months and years could be up to 90% of the population.

## Protection Endpoints

Most policy prescriptions are general in nature, consisting of immediate steps—for example, passing enabling legislation, appointing the right people to government positions, hiring staff at utilities, and establishing organizational processes. Of course, none of these intermediate steps

are actual cybersecurity protections. In evaluating progress to date ("what has been done") and what could be done, it is helpful to instead examine specific and tangible measures, or "protection endpoints."

## What Has Been Done

The following are examples of specific cybersecurity measures that have been taken by some utilities:

- Limiting physical access to key computer systems.
- Firewalls (or "electronic security perimeters") between utility computer systems and the public internet or between Operational Technology and Information Technology.
- Monitoring and logging of outgoing, incoming, and internal network traffic.
- Scanning and monitoring of computer systems for malware infections.
- Sharing of information on malware infections and other cyberattack methods among utilities and government agencies.
- Two factor authentication for remote access to key computer systems, requiring (1) a password and (2) possession of a physical device such as a cell phone.
- Stocking of spares for equipment that may be damaged in a cyberattack, such as large power transformers.
- Automated and real-time situational awareness and defense, as implemented in the Cybersecurity Risk Information Sharing Program (CRISP) of the U.S. Department of Energy and national laboratories.
- Disconnection of Operational Technology from Information Technology, or disconnection of Operational Technology from the public Internet—so called "air gapping"—as has been done at some U.S. nuclear power plants.
- Letting of a U.S. government contract for a resilient telecommunications network, "FirstNet," that can be used during cyberattack on critical infrastructure.

## What Could Be Done

Here are examples of cybersecurity measures have not been implemented by most utilities and their equipment vendors, but have been proposed:

- Reversion to analog (non-computer-based) control, or maintenance of redundant analog systems in older grid facilities, as proposed by some in Congress.
- Reversion to manual operation for the very most critical grid facilities, such as very large substations in key locations, as proposed by some in Congress.
- Use of one-way data flow devices—so-called "data diodes," as proposed by the U.S Department of Homeland Security.
- Use of specially designed hardware protective devices—an example being "Aurora" protective devices selectively installed at substations supplying power to military bases, as proposed and funded by the U.S. Department of Defense.

- Redesign of critical grid components, such as Programmable Logic Controllers (PLC), to eliminate security vulnerabilities, as proposed by the Open Process Automation Forum.
- Establishment of supply-chain certification to avoid the possibility of built-in malware, as proposed by the Federal Energy Regulatory Commission (FERC) to the delegated standard-setting organization, the North American Electric Reliability Corporation.
- Encryption of electric grid communications, including communications between control centers and transmission substations, as proposed by the Foundation for Resilient Societies in its September 2015 docket comments to FERC.[9]
- Required electric utility detection, reporting, mitigation, and removal of malware infections, as proposed by the Foundation for Resilient Societies in its January 2017 Petition for Rulemaking to FERC.[10]
- Establishment of a 24/7 nationwide monitoring capability to detect and defend against coordinated cyberattacks, as proposed by George Cotter, former Chief Scientist of the National Security Agency.

## Pathways to Protection

Even the best ideas for cybersecurity protection need societal mechanisms to ensure their widespread implementation. Potential mechanisms include legislation, executive action, mandatory standards, industry standards, voluntary measures, and establishment of utility liability. If all the foregoing is too little or too late, cyber-deterrence against foreign adversaries is a last resort. To bolster deterrence and improve defense, the FY 2017 National Defense Authorization Act does require training of National Guard units for cyber protection of electric utilities and other infrastructures.

### Legislation

Congress has attempted cybersecurity protection through legislation, but results have been mixed, because but federal agencies captured by industry interests can delay, water-down, or block implementation. Recent legislation has been weak, mostly establishing mechanisms in support of voluntary measures, such as "information sharing." Congress wisely included provisions in the Energy Policy Act of 2005 to protect electric grid "communication networks" against "cybersecurity incidents," but a decade later these provisions have not been implemented in mandatory regulation by the FERC.

---

[9] Foundation for Resilient Societies, "Comments of the Foundation for Resilient Societies," FERC Docket No. RM15-14-000. September 21, 2015. Accessed March 27, 2017. http://www.resilientsocieties.org/uploads/5/4/0/0/54008795/docket_rm15-14-000_resilient_societies_cybersecurity_20150921.pdf .

[10] Foundation for Resilient Societies, "Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System." FERC Docket No. AD17-9. January 13, 2017. Accessed March 27, 2017. http://resilientsocieties.org/uploads/5/4/0/0/54008795/resilient_societies_petition_for_rulemaking_ad17-9.pdf .

In the Cybersecurity Act of 2005, Congress encouraged information sharing between the government and utilities by eliminating liability, but placed no specific cybersecurity requirements upon utilities. Utility accountability measures are weak or nonexistent. In the Fixing America's Surface Transportation Act (FAST Act) of 2015, Congress provided for centralized command and control at the U.S. Department of Energy (DOE) during grid emergencies. The Fast Act also requires a DOE plan for a Strategic Transformer Reserve. At the writing of this document, DOE has gone nine months past the statutory deadline without a final rule on grid emergencies. Under that Act, the Secretary of Energy was designated as the principal coordinator for cyber security in the energy sector.

Because state legislatures are heavily lobbied by electric utilities, few states have passed cybersecurity legislation for their intrastate portions of the U.S. electric grid.

## Executive Action

The some of the best opportunities for executive action could be alignment of the administration appointments with the imperative of grid cybersecurity. Important appointments at the working level within the federal government include:

- Assistant Secretary for the Office of Electricity Delivery and Energy Reliability (OE) at DOE
- Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD) at DHS
- Under Secretary for the National Protection and Programs Directorate (NPPD) at DHS
- Assistant Secretary for Infrastructure Protection at DHS
- Assistant Secretary for Homeland Defense at DoD

It is critically important to appoint a competent official as Assistant Secretary for Electricity Delivery and Energy Reliability at DOE. This office should be the primary advocate and executive for electric grid resiliency and security within the executive branch. Because the Department of Defense and intelligence agencies have leading edge cyber protections in place, that Department can also assist and coordinate with DOE.

Since the 9/11 attacks heightened awareness of foreign threats to the American homeland, Presidents of both parties have issued a string of Executive Orders and Directives for cybersecurity of critical infrastructure, including the electric grid. The most relevant include:

- Presidential Policy Directive 41 — United States Cyber Incident Coordination (July 2016), establishing principles for federal government response to both government and private sector incidents.
- Presidential Memorandum— Establishment of the Cyber Threat Intelligence Integration Center (February 2015)
- E.O. 13691, Encouraging Private-Sector Cybersecurity Collaboration (February 2015), establishing collaboration and information sharing between the private sector and government

- E.O. 13636, Improving Critical Infrastructure Cybersecurity (February 2013), requiring the National Institute of Standards and Technology to establish a cybersecurity framework.
- Presidential Policy Directive (PPD) 21 - Critical Infrastructure Security and Resilience (February 2013), establishing national policy on critical infrastructure security and resilience.
- HSPD-7, Homeland Security Presidential Directive No. 7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003), assigning the Department of Homeland Security responsibility for coordinating infrastructure protection.

Significantly, these executive orders and directives prescribe government actions, but do not place mandatory requirements upon electric utilities, nor provide cost-recovery mechanisms.

### Mandatory Standards

The Energy Policy Act of 2005 established a system of mandatory standards for the Bulk Power System, electric generators and the high-voltage portion of transmission systems. Under the Act, federal rulemaking is managed by the Federal Energy Regulatory Commission, a regulator principally charged with economic regulation of energy infrastructure. Per the Act, detailed standard-setting has been delegated to an industry-managed "electric reliability organization" or ERO.

A previous utility trade association, the North American Electric Reliability Corporation (NERC), has been selected by FERC as the ERO. Standard-setting at NERC is governed by vote of ballot bodies, with most votes controlled by electric utilities. FERC has a practice of accepting NERC's weak first-round cybersecurity standards and trying for better standards in subsequent editions. Thus, marginal improvements in standards require years of negotiation—meanwhile grid vulnerabilities persist.[11] Fundamentally, utilities have resisted strong cybersecurity standards because the Energy Policy Act did not provide mechanisms for cost recovery for large segments of electric utilities—most importantly, electricity generators.

State PUC members often have strong ties to electric utilities and their law firms. Were state legislatures to pass laws requiring inconsistent standards for grid cybersecurity but lacking explicit funding mechanisms, implementation in regulation will likely follow the pattern of delay and minimization seen at the federal level.

### Process Industry Standards

For industrial process control systems, including control systems used in the electric grid, the leading standard-setting body is the International Electrotechnical Commission (IEC). IEC has initiatives to build cybersecurity into the basic building blocks for control systems. A new

[11] Conklin, W.A., "Keeping the Lights On: Cybersecurity and the Grid," *Forbes*, February 29, 2016. Accessed March 31, 2017. http://www.forbes.com/sites/uhenergy/2016/02/29/keeping-the-lights-on-cybersecurity-and-the-grid/#238e192988e2.

industry initiative with many large companies participating, the Open Process Automation™ Forum, aims to improve cybersecurity for a variety of process industries, including electric utilities. In the long-term, industry initiatives such as these will form a stronger technical basis for "built-in" cybersecurity.

## Voluntary Measures

As part of President Obama's Executive Order (EO) 13636 in February 2013, the National Institute of Standards and Technology (NIST) was tasked to work with industry to develop a voluntary framework for cybersecurity. The result was the February 2014 ""Framework for Improving Critical Infrastructure Cybersecurity." Among cybersecurity practitioners, this framework has gained wide acceptance as the premier methodology for good cybersecurity practices, applicable across a wide variety of industries. In January 2014, NIST released a draft update to its framework which is currently out for public comment.

Additional industry-specific voluntary measures have been undertaken by NERC. These include operation of an Electricity subsector Information and Analysis Center (E-ISAC), and annual grid security conference (GridSecCon), and a biennial grid security exercise, GridEx. The Electric Sub-sector Coordinating Council (ESCC), a voluntary association of utility representatives and trade associations, provides a forum for industry information sharing.

## Financial Liability and Insurance

In nearly every state, utilities have been protected from financial liability due to blackout, except in cases of gross negligence. The principal mechanism for this protection has been the system of tariffs approved by state PUCs or by Regional Transmission Organizations, which have the force of law. This liability protection has reduced incentives for better cybersecurity. Recently, the State of Ohio passed legislation which prohibits the PUC from granting liability protection in tariffs. Were utility liability to be established in more states, underwriting and risk assessment by insurance companies could be incentives for better cybersecurity. Appropriate disclosure of cybersecurity risks in Securities and Exchange Commission filings could also motivate utilities for better security.

## Cyber Deterrence

In February 2017, the Defense Science Board published its final report of the Task Force on Cyber Deterrence. Notable findings include:

- "Major powers (e.g., Russia and China) have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack, and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks."
- "Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures."
- "Bolstering the U.S. cyber deterrence posture must be an urgent priority."

It is notable that an official body of the U.S. Government, the Defense Science Board, has conceded that cybersecurity of critical infrastructure, including the electric grid, is so weak that deterrence must be principally relied upon for the next decade or more.

## Costs and Funding

The cost of improving cybersecurity protection for the electric grid will be substantial. The most vulnerable equipment—control systems designed without integrated security protection—is decades old and must be replaced. Some cost-saving measures, such as internet remote access to substation equipment, must be circumscribed or eliminated. Additional protective equipment and organizational processes will be required; in many cases, the cost of integrating new equipment will be many times the purchase price.

Currently, most cybersecurity measures are funded through utility operating budgets. Within current regulatory structures, it is difficult for utilities to recover their cybersecurity costs. Going forward, these four mechanisms might fund better cybersecurity:

- Recovery of reasonable and justifiable costs through the rate-making and tariff processes.
- Tax credits for high-priority and specific cybersecurity improvements.
- Direct appropriations by state and federal legislatures.
- Subsidized leasing of "dark fiber" telecommunications systems that meet cybersecurity standards already employed for the Department of Defense and the intelligence agencies.

## Policy Recommendations

We propose the following policy recommendations to enhance cybersecurity of the electric grid:

1. Congress and the President should pass legislation establishing specific timelines and accountable organizations for cybersecurity protections; in the past, legislation lacking timelines and accountability has not been implemented or implemented with long delays.
2. Setting of mandatory cybersecurity standards should be performed by government agencies, not industry groups; this will require changes by Congress to the Energy Policy Act.
3. Legislative and regulatory mechanisms to fund cybersecurity improvements at utilities must be established; without sufficient funding, cost-saving measures enabled by internet connections will nearly always take priority over cybersecurity.
4. Voluntary measures such as the NIST Frameworks should be supported by government, but they should substitute for mandatory and funded cybersecurity protections.

5. A government-managed process for supply-chain certification to avoid the possibility of built-in malware; the U.S. Food and Drug Administration process to avoid food contamination might be a regulatory model.
6. U.S. Government Accountability Office (GAO) review of the recently awarded FirstNet contract to AT&T to prevent minimizing of technical requirements, e.g., exclusion of "all hazards" protection for cyberattack, physical attack, and nuclear electromagnetic pulse.
7. A policy of cyber-deterrence should not be a long-term replacement for tangible cybersecurity protections.

## Cybersecurity Outlook

The near and mid-term cybersecurity outlook for the U.S. electric grid is fair to poor. Electric grid cybersecurity is a race between technological innovations that increase vulnerability, on one side, and costly protective measures on the other. Because utilities are under constant pressure by regulators and customers to reduce costs and improve service, and because a grid cyberattack has not yet occurred in the United States, the business rationale for cybersecurity protection is uncertain. Funding mechanisms for cybersecurity protections are lacking. Legislation, executive actions, mandatory standards, industry standards, and voluntary actions are having marginal impact in the face of every-stronger economic incentives for internet connections. Absent greater determination for policy reform by the President, Congress, and grid regulators it is unlikely that comprehensive cybersecurity protections will be implemented in advance of a costly and life-threatening wide-area blackout.

**Background on the Foundation Resilient Societies**

*The Foundation for Resilient Societies is a non-profit dedicated to cost-effective protection of critical infrastructures from infrequently occurring natural and man-made disasters. Resilient Societies is the only non-profit that consistently participates in FERC rulemakings for grid security standards. For more information, see our website at [www.resilientsocieties.org](http://www.resilientsocieties.org).*

## References

1. U.S. Congress. House. Committee on Armed Services. Threat Posed by Electromagnetic Pulse Attack (EMP) Attack. Hearing held July 10, 2008. 110th Cong., 2d sess., 2008. pp. 8-9. Accessed March 27, 2017. https://fas.org/irp/congress/2008_hr/emp.pdf.
2. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* Report. U.S. Department of Energy and North American Electric Reliability Corporation. June 2010. Accessed March 27, 2017. https://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.
3. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." Report. February 12, 2014. Accessed March 27, 2017.

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

4. Hayden, Michael, Hebert, Curt, Tierney, Susan. *Cybersecurity and the North American Electric Grid*. Report. Bipartisan Policy Center's Electric Grid Cybersecurity Initiative. February 2014. Accessed March 27, 2017. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20.
5. U.S. Department of Energy. *Large Power Transformers and the U.S. Electric Grid.* Report. April 2014. Accessed March 27, 2017. https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf.
6. Michael S. Rogers, Director, National Security Agency, and Commander, U.S. Cyber Command, "Cybersecurity Threats: The Way Forward," before the U.S. House Energy Committee. Testimony. November 20, 2014. Accessed March 30, 2017. https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml .
7. Cambridge Centre for Risk Studies, University of Cambridge. *Business Blackout; The insurance implications of a cyber attack on the US power grid*. Report. May 2015. Accessed March 27, 2017. https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
8. Campbell, Richard J. "Cybersecurity Issues for the Bulk Power System." Congressional Research Service report, June 10, 2015. Washington D.C. Accessed March 27, 2017. https://fas.org/sgp/crs/misc/R43989.pdf.
9. Foundation for Resilient Societies, "Comments of the Foundation for Resilient Societies," FERC Docket No. RM15-14-000. September 21, 2015. Accessed March 27, 2017. http://www.resilientsocieties.org/uploads/5/4/0/0/54008795/docket_rm15-14-000_resilient_societies_cybersecurity_20150921.pdf .
10. Koppel, Ted. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. Crown; 1st edition (October 27, 2015).
11. U.S. Department of Energy. *Quadrennial Energy Review: Second Installment.* Report. January 2017. Accessed March 27, 2017. https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment.
12. SANS Institute and Electricity Information Sharing and Analysis Center (E-ISAC). *Analysis of the Cyber Attack on the Ukrainian Power Grid; Defense Use Case*. Report. March 18, 2016. Accessed March 27, 2017. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
13. Conklin, W.A., "Keeping the Lights On: Cybersecurity and the Grid," I, February 29, 2016. Accessed March 31, 2017. http://www.forbes.com/sites/uhenergy/2016/02/29/keeping-the-lights-on-cybersecurity-and-the-grid/#238e192988e2 .
14. Foundation for Resilient Societies, et. al., "Joint Request and Motion of Foundation for Resilient Societies, Isologic, LLC and Applied Control Solutions, LLC for the Commission to Reopen the Evidentiary Record In Docket Rm15-14-000 As Authorized By FERC Rule 716."

FERC Docket No. RM15-14-000. March 29, 2016. Accessed March 27, 2017. http://resilientsocieties.org/images/RM14-15-000_Resilient_Societies_Sept_8_2014.pdf.

15. Fairley, Peter. "Upgrade Coming to Grid Cybersecurity in U.S." IEEE Spectrum, April 20, 2016. Accessed March 27, 2017. http://spectrum.ieee.org/energy/the-smarter-grid/upgrade-coming-to-grid-cybersecurity-in-us.
16. Shea, Daniel. "State Efforts to Protect the Electric Grid." Report. National Conference of State Legislatures. April 2016. Accessed March 27, 2017. http://www.ncsl.org/Portals/1/Documents/energy/ENERGY_SECURITY_REPORT_FINAL_April2016.pdf.
17. North American Electric Reliability Corporation. "CIP-005-5 — Cyber Security — Electronic Security Perimeter(s)." Reliability Standard. June 1, 2016. Accessed March 27, 2017. http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf.
18. Nuclear Energy Institute, "Cyber Security for Nuclear Power Plants." Policy Brief. July 2016. Accessed March 27, 2017. https://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants.
19. Tehan, Rita. "Cybersecurity: Legislation, Hearings, and Executive Branch Documents." Congressional Research Service report, October 21, 2016. Washington D.C. Accessed March 27, 2017. https://fas.org/sgp/crs/misc/R43317.pdf.
20. Draffin, Cyril W. *Cybersecurity White Paper*. White Paper. MIT Energy Initiative Utility of the Future. December 15, 2016. Accessed March 27, 2017. https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf.
21. Smith, R., "Fears Over U.S. Power Grid; Recent cyberattacks in Ukraine raise alarms over vulnerability of infrastructure here," *Wall St. Journal*, December 31, 2016.
22. BBC News, "Ukraine power cut 'was cyber-attack," January 11, 2017. Accessed March 31, 2017. http://www.bbc.com/news/technology-38573074 .
23. Foundation for Resilient Societies, "Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System." FERC Docket No. AD17-9. January 13, 2017. Accessed March 27, 2017. http://resilientsocieties.org/uploads/5/4/0/0/54008795/resilient_societies_petition_for_rulemaking_ad17-9.pdf.
24. U.S. Government Accountability Office. *Federal Efforts to Enhance Grid Resilience*. Report. GAO-17-153: Published: January 25, 2017. Publicly Released: Feb 24, 2017. Accessed March 27, 2017. https://www.gao.gov/products/GAO-17-153.
25. James N. Miller, James R. Gosler, et al., *Task Force on Cyber Deterrence*, Report. February 2017. Accessed March 31, 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf .
26. The Open Group. "The Open Process Automation™ Forum." Website. Undated. Accessed March 27, 2017. http://www.opengroup.org/open-process-automation/forum.