Protecting America's Electric Grid Against Physical Attack

March 2017

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

Executive Summary

The widely distributed and often unattended nature of America's electric grid leaves it open to physical attack. A coordinated physical attack 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.[1] Such a blackout could result in the death of up to 90% of America's population in the first twelve months.

It is not possible to guard or otherwise physically protect all electric grid facilities. For example, it is impossible to guard the pylons of long-distance transmission lines running through remote areas. However, it is possible to protect the most critical electric grid facilities such as master control centers, large generation plants, and the small number of critical substations that are epicenters for the transmission of high voltage electricity.

Because all utilities are electrically interconnected, an attack on an unprotected facility may produce an imbalance in power that will surge through the network, causing a cascading collapse. When a cascading collapse occurs, power surges can cause permanent damage to hard-to-replace grid equipment; much of this equipment is manufactured in foreign countries with replacement lead times in excess of one year.

In April 2013, unknown parties attacked a critical electric grid substation in San Jose, California that supplies the majority of power for Silicon Valley and San Francisco. A wide area blackout was narrowly avoided. This and other grid attacks have been wake-up calls for action to protect America's electric grid from physical attack.

Significant government action to-date consists of a mandatory standard for physical security of electric grid facilities ordered by the regulator of the high-voltage portion of the U.S. electric grid, the Federal Energy Regulatory Commission (FERC). Since passage of this standard, utility awareness of physical vulnerabilities has increased, but protection of grid facilities has improved only marginally.

FERC's physical security standard places no specific requirements upon utilities; instead, it requires paper security plans that can be approved by peer utilities. The FERC security standard exempts all electric generation plants, regardless of size or significance. Additionally, some of the most important master control centers are exempted from the FERC security standard.

Societal pathways to better physical security may include: legislation; executive action; mandatory standards; use of innovative security technologies; voluntary measures by utilities;

[1] A May 2013 study conducted by the Federal Energy Regulatory Commission (FERC) and leaked to the *Wall Street Journal* concluded that a well-planned physical attack on just nine transmission substations would cause a nation-wide grid outage that would take 18 months to restore. See Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack." *Wall Street Journal*, March 14, 2014. Accessed March 27, 2017. https://www.wsj.com/articles/SB10001424052702304020104579433670284061220 .

establishment of financial liability for utilities; and protection by government authorities at times of increased threat, including use of National Guard units for physical and cyber-defense of civilian infrastructure.

Utilities are likely to resist physical security improvements unless recovery of costs can be assured. Potential mechanisms of funding include assessments upon ratepayers, tax credits, and direct appropriations by state or federal legislatures.

Recognizing the severity of the threat, and despite a lack of mandatory requirements, larger investor-owned utilities have physically protected the most critical electric grid facilities—including important control centers, generation plants, and transmission substations. But physical protection remains weak in most locations, especially for utilities that lack mechanisms for cost recovery. As a result, the risk of wide-area blackouts from physical attacks looms large.

Physical Attack Threat

The electric grid in the continental United States is a massive machine containing 450,000 miles of high-voltage transmission lines, 5.5 million miles of low-voltage distribution lines, 7,000 generation plants, 55,000 transmission substations, 200 transmission control centers, and 12 master control centers. Many grid facilities are in rural areas without significant police presence. Because of the distributed nature of America's electric grid, it is impossible to comprehensively protect all facilities from physical attack.

Types of Grid Facilities

The vast majority of electricity is generated in large-scale electric generation plants (so-called central stations), although some is generated in distributed solar panels and wind farms. Once generated, electricity is stepped up to high voltage and routed through a network of transmission lines. Near homes and businesses, electricity is stepped down to lower voltage at substations and distributed through local lines. The electricity network is managed by centralized control facilities that communicate with the various components through telecommunications. Utilities have used leased telephone lines for slower communications. When faster communications is required, utilities have often established their utility-owned data links.

Electric Generation Plants

Most electric generation facilities are staffed; notable exceptions are wind turbines, small solar farms, and small hydroelectric facilities. Large generation plants may have a dedicated security force, while smaller plants may assign subsidiary security duties to employees on-site.

Nearly all generation plants have some kind of perimeter security; chain-link fences topped by barbed wire are the most common type of protection. In urban areas, generation plants can be protected by brick or cinderblock walls topped by barbed wire. Larger plants often have secure parking lots with access controlled by staffed guard stations. It is common for generation plants to have closed-circuit television cameras monitoring their security perimeters. At some plants,

transmission switchyards and communications facilities are located outside the main security perimeter.

In rural areas, generation plants are often surrounded by large acreage where access can be monitored and restricted. In urban areas, smaller security perimeters for generation plants are often directly adjacent to public thoroughfares including roads and waterways.

A significant proportion of generation plants have commercial or public access to nearby areas. Because of the necessity of water for cooling, thermal generation plants are commonly adjacent to rivers, lakes, and bays that are used for shipping and recreation. Hydroelectric facilities may have scenic overlooks, visitor parking lots, or other areas to facilitate viewing. Some utilities have adapted a practice of granting public access to their land—fishing piers, picnic areas, boat ramps, and hiking paths being examples of public accommodations. In Florida, utilities have established viewing areas to watch manatees attracted by the warm water discharge. All of these public access mechanisms complicate defense against physical attack.

Fossil-fueled generation plants are often large structures with long runs of exposed piping and conduits. In many cases, it is not possible to cost-effectively protect large generation plants against kinetic attack by rifle, rocket propelled grenade, mortar, or vehicle bombs. In recent years, remotely controlled drones have become another means of potential physical attack on generation plants.

Nuclear power plants have special physical security, above and beyond other generation plants. Nearly all nuclear power plants within the United States have been constructed in less populated areas where access can be better controlled. All nuclear power plants have well-established standoff perimeters, dedicated guard forces, and hardened containment vessels. The U.S. Nuclear Regulatory Commission periodically conducts force-on-force exercises to test physical security at nuclear power plants; and shares "lessons learned" with nuclear plant licensees, but not with fossil-fuel generating facilities.

High-Voltage Transmission Lines

Within the United States, there are approximately 500,000 miles of high-voltage transmission lines and approximately 55,000 transmission substations, typically operating at voltages over 100 kV. Transmission lines can run both overhead and underground.

By their very nature, transmission lines are vulnerable to physical attack. Potential modes of attack including dropping conductive materials across the lines, shooting out ceramic insulators, weakening transmission poles or metal pylons so they will collapse, and compromising underground cable vaults.

Most transmission lines have redundant paths; therefore, under the "N-1" planning criteria of utilities, loss of the single transmission line should not cause a blackout. If a transmission line is brought down by physical attack, utilities commonly have line crews and replacement parts on

standby, because weather-induced events can bring down transmission lines and require quick repair capability.

High-Voltage Transmission Substations

Approximately 2,500 high-voltage transmission substations in the United States contain large power transformers that are essential for long distance transmission of electricity. High-voltage transmission substations are attractive targets—an attack on a critical substation could cause cascading grid collapse or long-term power deficits over large geographic areas. The vast majority of substations are unmanned facilities protected by chain-link fences. A significant number of substations are in remote locations with sparse law enforcement.

Since the passage of FERC's mandatory standard for physical security, ballistic barriers have been erected around some substations or around the most critical equipment in substations, such as extra high-voltage transformers. Critical substations often have closed-circuit television cameras and sometimes acoustic gunfire detection systems connected to centralized security monitors.

Distribution Lines and Substations

In the United States, there are 5.5 million miles of distribution lines and associated distribution substations, typically operating at voltages less than 100 kV. Distribution lines and substations serve end-consumers of electric power. Most often, the power running through any particular distribution line or substation serves a small percent of the population of a state or region. As a result, while an attack on distribution lines and substations will cause inconvenience for particular power consumers, it is unlikely to cause cascading outage or wide-area impact.

Control Facilities

When the electric grid was originally constructed, control devices such as substation switches and circuit breakers were operated by personnel on-site. Collection of data on grid operating conditions—voltage, current, and frequency measurements, for example—was also done manually. In a long evolution, starting in the 1920's, control signals began to be transmitted to and from centralized control facilities. Operators in the control centers would read the system state data and then remotely actuate switches and other control devices. Expanding availability of cheap telecommunications and microprocessor control devices in the post-World War II period accelerated the use of centralized control facilities.

Centralized control facilities are now critical to grid operation. Control facilities at electric utilities manage the operation of hundreds or even thousands of grid substations each. The vast majority of grid substations are completely automated, with no staff on-site. Because disruption of a control facility can disrupt grid operations over a wide area, these facilities are likely targets for physical attack.

For the major control facilities, it is common for there to be a primary location and a backup facility. (A few utilities have tertiary facilities.) Primary and backup facilities can be located in close proximity, to allow operators to quickly move from one location to another. A more

secure practice is to separate primary and secondary control facilities by dozens or hundreds of miles, with 24/7 staffing at each location.

Security for electric grid control facilities varies widely. Some control facilities are contained within large acreages with double layers of fencing, closed-circuit television cameras, and guard forces. Other control facilities are contained in multitenant office buildings with only perfunctory security. Control facilities constructed before the current era of terrorist threats are sometimes adjacent to publicly accessible parking lots.

Without functioning control facilities during a blackout, utilities would be forced to dispatch technicians to grid substations to manually operate switches and other control devices. Communication with technicians would be by landline telephone or cell phone (if the commercial telecommunications system is working) or by radio. Speed and precision of grid control would be greatly hampered without control facilities. Because an attack on a control facility can disrupt grid operations over a wide area, control facilities have become targets for physical attack.

Communications Facilities

Geographically distributed electric grid facilities combined with centralized control requires reliable communications. In original control schemes, use of leased commercial telephone lines was common. As more sophisticated control systems required faster communications, utilities began to use microwave radio and dedicated fiber optics. In recent years, communications have been augmented by meshed cellphone networks. Utilities often use multiple and redundant telecommunications paths.

Nodes for communication facilities, such as microwave towers, are commonly protected by chain link fences. Fiber optic communications requires regeneration facilities every few hundred miles; these facilities are commonly located in windowless huts protected by chain link fences. Local ordinances commonly require security fencing for cell phone towers and associated equipment.

Physical attack on any single communications node is unlikely to bring down an electric grid over a wide area. However, if attackers have detailed knowledge of a utility's telecommunications network scheme, and target multiple critical nodes, such an attack could have major impact.

Co-Location of Electric Grid Facilities

Generation plants and transmission lines (including their substations) require local permitting and federal government approval for environmental impact. Moreover, local residents commonly resist construction of transmission facilities—especially high voltage transmission lines that can be unsightly. Increasingly, people living or working next to high voltage transmission lines fear health effects from electromagnetic radiation. To ease federal government approval and local permitting, utilities often take an easier route by expand existing facilities—for example, by adding generation units to an existing plants, siting new

generation plants adjacent to existing plants, and adding new lines and transformers to existing substations. All of these practices concentrate physical security risks.

Attack Scenarios

An effectively executed and coordinated physical attack could cause long-term grid outage over large geographic areas. At any point in time, the production of electricity must exactly balance with the consumption of electricity. Physical attack can upset this balance by interrupting electricity generation, transmission, distribution, and control. For example, a physical attack on a large generation facility can cause a destabilizing shortage of electricity. Attack on a key substation can interrupt transmission of electricity, causing a surplus of electricity upstream and a deficit of electricity downstream. Attack on a control facility can alter generation plant dispatch and transmission line routing, causing some lines to be overloaded. When electricity supply and consumption does not match, or when lines are overloaded, a cascading collapse can occur, affecting large regions. Damage to control facilities can cause loss of situational awareness necessary for rapid power restoration.

Security contingency planning criteria for electric grid facilities is commonly "N-1," meaning loss of a single component will not cause grid collapse. However, due to the common practice of co-locating electric grid facilities, a single attack on co-located or adjacent facilities can cause loss of multiple components, risking cascading collapse. Even if facilities are not co-located, a coordinated physical attack greatly increases the risk of cascading collapse.

Asymmetric Nature of Physical Attack

A physical attack on the electric grid does not require sophisticated planning, special skills, or hard-to-obtain weapons. Planning for an attack is made easier by extensive and publicly available data for electric grid facilities and operations. Using Google Maps (including overhead satellite images and Street View pictures), operatives anywhere in the world can conduct pre-attack reconnaissance. Extensive data on generation plants, transmission lines, and power flows is publicly available, because efficient operation of wholesale power markets requires its continual disclosure. Millions of people around the world have military training or other instruction on the use of weapons. Rifles are easily available in the U.S. at retail gun stores, gun shows, and on the black market. Foreign operatives infiltrated through U.S. borders could attack grid facilities, damaging hard-to-replace equipment and permanently collapsing the electric grid.

Combined Physical and Cyber Attacks

The potential harms of physical attacks on critical grid facilities should not be assessed in isolation. Physical intrusions may be a "cover" for injection of cyber-malware into grid control systems, including "zero day" capabilities that could be activated as part of a later cyber attack. In recent years, unauthorized entry into electric substation facilities has increased; and at a PG&E facility near Bakersfield, California, a Supervisory Control and Data Acquisition (SCADA) system was stolen, which raises concerns about reverse engineering for later cyber attack.

Threat assessments should include coordinated attacks, including physical attack, denial of service attack, offensive cyber attack, and other attack vectors.

Grid Restoration Challenges After Physical Attack

In addition to direct equipment damage, physical attacks may cause power surges as the grid collapses. Power surges, if not properly protected mitigated, can cause damage to critical grid equipment such as generators and transformers. Most large power transformers have unique designs. The lead time to order replacements for large transformers and generators is in excess of one year. Nearly all large power transformers are manufactured outside of the United States.

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 batteries typically last eight hours. Diesel fuel for backup generators at control facilities is also limited, with typical duration of a few days. Utilities commonly have pre-established contracts for resupply of diesel fuel, but during an emergency, delivery may not be assured.

After a physical attack, utilities may be forced to dispatch technicians to substations to manually close circuit breakers and switches, time-consuming steps. 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: Physical Attacks on Grid Facilities

Minor physical attacks on electricity facilities have been a long-time nuisance for grid operators. For example, vandals commonly use rifles to shoot out ceramic insulators on power lines. However, in recent years there have been a number of physical attacks that demonstrate intent to cause wide-area blackouts within the interconnected U.S.-Canada electric grid.

Metcalf Attack

In the early morning of April 16, 2013, a sophisticated attack outside San Jose California demonstrated vulnerabilities of grid substations. The target was the Metcalf substation supplying much of the power for Silicon Valley and the city of San Francisco. As population in the San Francisco Peninsula grew, and polluting power plants within the city limits were shut down, more and more power was routed through this single substation, causing it to be a critical failure point.

At 12:58am, unknown gunmen first cut communications cables to the Metcalf substation. The attackers then used an AK-47 rifle to shoot out transformer radiators. At 1:50 am a utility video camera caught a flashlight signal that may have marked the end of the attack. At 1:51 am police arrived on the scene, apparently after a lookout had warned the attackers to flee.

Radiators for 17 out of 21 transformers had been shot out. Loss of just one more transformer would have caused a wide-area blackout for the San Francisco Peninsula. Because the attackers missed cutting a communication cable for transformer telemetry, grid operators observed the substation transformers overheating and were able to take the transformers off-line before permanent damage occurred.

At the time of the Metcalf attack, Jon Wellinghoff was chairman of FERC. As the lead federal official for electric reliability, Mr. Wellinghoff had previously warned about the danger of physical attack—and now a significant attack had occurred. Mr. Wellinghoff assembled an investigation team that included Navy Seals and personally toured the attack site. The investigation revealed that the attackers had used military-type techniques.

Electric utilities and complicit law enforcement initially tried to cover up the gravity of the Metcalf attack. Within weeks of the attack, Mr. Wellinghoff announced his early resignation for undisclosed reasons, but stayed on the job until November 2013.

In February of 2014, an article in the *Wall Street Journal* disclosed details of the Metcalf attack. A follow up article, based on leaked information, disclosed that FERC had conducted a study of the U.S. grid in May of 2013. The FERC study had concluded attacks on only nine grid substations could cause a continent-wide blackout lasting 18 months. Mr. Wellinghoff had provided the FERC study to Congress, but no legislative action had been taken, nor had there been public oversight hearings.

Liberty Substation Attack

On November 15, 2013 an unknown attacker cut fiber optic cables for communications to the Liberty Substation in Buckeye, Arizona. This substation is important for the supply of electricity for California. Investigation by a utility technician found the perimeter fence cut and the steel door to the control hut breached. Within the control hut, computer cabinets had been pried open.

On January 30, 2014, the Liberty station suffered another attack by two men caught on a security camera. The men cut the gate lock and then left when they failed to cut power to a security trailer.

Hydro-Quebec Transmission Line Attack

On December 4, 2014, an attacker used a small airplane to drop objects on two 735 kilovolt transmission lines for Hydro-Québec, shorting out the lines. The attack caused a blackout for 188,000 customers in the area of Montreal, Quebec.

The Stakes for America

Contemporary American society depends on continuous electric power. An effectively planned and executed physical attack 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 could result. Gas station fuel pumps and traffic control will fail, preventing evacuation of major metropolitan areas.

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. Approximately 100 nuclear power plants in the United States have spent fuel pools that could catch fire during long-term loss of grid power.

During the 2011 Fukushima disaster in Japan, emergency managers feared that the spent fuel pool at Fukushima Unit No. 4 had gone dry and might catch fire, nearly causing an order for the evacuation of Tokyo.

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 R. Graham, former Presidential science advisor, casualties in the aftermath of a nationwide infrastructure outage could be as high as 90% in the first twelve months.

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

What Has Been Done

The following are examples of specific physical security measures that have been taken by some utilities and government authorities:[2]

- Wire fences that allow external view of grid facilities, most often chain-link design
- Closed-circuit television cameras
- Guards at some larger generation facilities
- Open space perimeters around rural generation facilities

[2] For a recent survey of physical protection practices by electric utilities, see "The State of Physical Grid Security." Report. *Utility Dive*. 2015. Accessed March 27, 2017. http://www.utilitydive.com/library/the-state-of-physical-grid-security-2015-report/ .

- Backup control facilities
- Redundant transmission lines and substations
- Stocking of spares, especially spares for large power transformers
- Temporary dispatch of police to guard the most critical grid facilities

What Could Be Done

The following are examples of stronger physical security measures that have not yet been implemented by most utilities and government authorities:

- Opaque fencing to prevent rifle sighting of key equipment
- Ballistic barriers around key equipment, such as large power transformers
- Dedicated, single-occupant buildings for control facilities
- Restricted parking adjacent to key facilities, especially control facilities
- Armed guards at the most critical facilities, including control facilities, transmission substations, and large generation plants
- Placing the most important master control facilities within large, defensible perimeters—for example, on military bases
- Contingency planning for simultaneous loss of major generation plants and transmission lines, especially when multiple plants and lines are co-located
- Centralized reporting for 24/7 situational awareness of coordinated physical attacks
- Force-on-force exercises to practice defenses against attack

The following protective measures might be taken by government authorities:

- Improved control at borders with Mexico and Canada to prevent infiltration of foreign operatives
- Dispatch of local law enforcement or National Guard troops to guard the most critical grid facilities at times of increased threat
- Plans for quick dispatch of extra fuel for backup diesel generators, especially at control facilities

Pathways to Protection

Even the best ideas for physical security of the electric grid need societal mechanisms to ensure their widespread implementation. Potential mechanisms include legislation, executive action, mandatory standards, technological innovation, voluntary measures, establishment of utility financial liability, and government protection.

For physical attack, deterrence applied to foreign adversaries is a dubious solution. Physical attacks can be asymmetrical, not requiring the resources of a nation-state. Terrorist groups may not be deterred from physical attack by the threat of retaliation.

Legislation

In recent years, legislation proposing greater grid protections has become more common. The Fixing America's Surface Transportation Act (FAST Act) of 2015 contained two provisions relating to physical security of the electric grid. A provision for emergency grid orders allow the Secretary of Energy to exercise control over the electric grid during emergencies and also provides for prudent cost recovery by utilities for their expenses incurred in following such emergency orders. The FAST Act also requires the Secretary of Energy to develop a 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 emergency orders.

Legislation for physical security of electric utilities is an imperfect instrument, because there is great variety in electric grid configurations and utility business models. For example, municipal utilities may have to get approval to recover costs for physical security improvements from their ratepayers, i.e., residents within their community.

Executive Action

Some of the best opportunities for executive action could be alignment of the administration appointments with the imperative of electric grid security. 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
- 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 and resiliency-supportive official as Assistant Secretary for Electricity Delivery and Energy Reliability at DOE. This office should be the primary advocate for electric grid resiliency and security within the executive branch.

Executive orders are another means of executive action. Significant executive orders and directives relating to physical security of critical infrastructure, such as the electric grid, include:

- 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.

These executive orders and directives prescribe government actions, but do not place mandatory requirements upon electric utilities.

Mandatory Standards

Federal Energy Regulatory Commission (FERC) regulates physical security for the interstate electric grid, the so-called "Bulk Power System." FERC is a five-member independent commission appointed by the President and confirmed by the Senate. Ensuring grid security is a subsidiary duty for FERC and its busy commissioners. FERC processes over 1,000 orders per year; nearly all orders relate to economic regulation. Previous FERC Commissioners commonly have had revolving door relationships with state public utility commissions, utilities, law firms, and lobbying groups.

Per Section 215 of the Federal Power Act, FERC has delegated the setting of physical security standards to an industry-dominated body, the North American Electric Reliability Corporation (NERC). Prior to the Act, FERC was an industry trade association. NERC is governed by vote of its membership. A utility sector representation scheme for vote counting ensures that electric utilities control the affairs of NERC. Many key committee positions at NERC are held by employees of investor-owned utilities.

Twenty-three days after the Metcalf substation attack, a key NERC committee recommended elimination of its physical security standard then under development. Senior FERC officials witnessed the NERC committee vote to abandon an obviously-needed standard, but FERC as a body did not act to reverse NERC's action.

Only after a series of article in the *Wall Street Journal* in February and March of 2014 did FERC order NERC to set a standard for physical security.[3] [4] The FERC-approved physical security standards exempt all generation plants, regardless of size or significance. Additionally, a significant number of master control centers for regional reliability coordinators are exempted from FERC's physical security standard.

Generation plants in competitive power markets (about two-thirds of the U.S.) lack a mechanism for cost recovery of security improvements. Representatives of generator operators commonly serve on key NERC committees and standard drafting teams. For example, the chair and vice-chair of the standard drafting team for physical security were employed by Exelon and Dominion, respectively, two of the largest generator operators in the U.S.

Without legislative fixes to allow cost recovery for security improvements under the FERC-NERC system of standard-setting, any resulting standards are likely to exempt certain utility sectors and otherwise have weak requirements.

---

[3] Smith, Rebecca. "Assault on California Power Station Raises Alarm on Potential for Terrorism." *Wall Street Journal,* February 5, 2014. Accessed March 27, 2017. https://www.wsj.com/articles/SB10001424052702304851104579359141941621778.

[4] Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack." Wall Street Journal, March 14, 2014. Accessed March 27, 2017. https://www.wsj.com/articles/SB10001424052702304020104579433670284061220 .

For electricity distribution utilities operating within individual states, regulation is by public utility commissions. At the state level, there is often little or no regulation of grid security, including physical security. As with FERC, state public utility commissioners commonly have close relationships with electric utilities and their law firms.

At the state level, government officials often prioritize lower electricity rates over protection for infrequent events—defense against physical attack being an example. Military-type defense of the grid can be viewed by local officials as a responsibility of the federal government. State legislatures and public utility commissions commonly have shielded utilities from liability lawsuits, except in the case of gross negligence.

Technological Innovation

Hard-to-replace transformers are a key target for physical attack. Recognizing this vulnerability, in 2008, DHS initiated the Recovery Transformer program ("RecX") in conjunction with the Electric Power Research Institute (EPRI) and ABB. This mobile and interchangeable transformer can be more easily transported and installed in emergencies. In 2012, a prototype unit was successfully installed and tested at CenterPoint Energy in Texas. According to press reports, no production units for the RecX transformer have been ordered by utilities.

More recently, Siemens has designed a line of mobile resiliency transformers that are "plug and play" for a variety of substation configurations. In March 2017, the first production units were successfully installed by ConEdison in New York.[5]

Voluntary Measures by Utilities

Voluntary measures to improve physical security have been piecemeal. Recognizing that having spare transformers on hand will be critical to recovering from a physical attack, the electric utility industry has initiated a number of voluntary programs for stocking and sharing of spares. These include the Spare Transformer Equipment Program (STEP) of the Edison Electric Institute, Spare Equipment Database (SED) by NERC, Grid Assurance LLC, funded by a consortium of utilities, SpareConnect by the American Public Power Association, the FLEX program of the Nuclear Energy Institute, including spare equipment warehouses in Memphis, Tennessee, and near Phoenix, Arizona; and other trade associations, and Wattstock, a privately owned service.

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

[5] Siemens. "Siemens mobile transformers are increasing the stability of New York's power grid." News release, March 16, 2017. Accessed March 27, 2017. http://www.siemens.com/press/en/pressrelease/?press=/en/pressrelease/2017/energymanagement/pr2017030225emen.htm&content%5b%5d=EM .

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 liability shield has been the system of tariffs approved by state PUCs. These tariffs have the force of law. Liability protection for utilities has likely reduced incentives for better physical security.

Recently, the State of Ohio passed legislation which prohibits the state PUC from granting liability protection in tariffs. Were utility liability exposure to be established in more states, underwriting and risk assessment by insurance companies could be an incentive for physical security and insurance audits. Requiring disclosure of physical security risks in Securities and Exchange Commission prospectuses could also motivate utilities for better security.

Protection by Government Authorities

Because it is impossible to protect every grid facility from physical attack, prevention and effective defense against attacks must be a priority. To prevent infiltration of foreign operatives, border control is important. SWAT teams or other rapid response forces may be necessary to supplement local law enforcement, especially in rural areas with sparse coverage.

Costs and Funding

The costs of physical protection for grid facilities can be substantial—in the hundreds of millions or billions of dollars for large utilities. Currently, most expenditures for physical security must be recovered from ratepayers after approval by state Public Utility Commissions (PUC). Due to the cost-reduction focus at most PUC, and the rarity of high-consequence physical attacks, PUC can be reluctant to approve such expenditures. Merchant generation facilities often lack any mechanism for cost recovery of security improvements.

Going forward, these three mechanisms might fund better physical security:

- 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.

Policy Recommendations

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

1. The President should initiate development of a national strategy for physical security of the U.S. electric grid, with specific responsibilities and actions by government authorities that can be implemented by executive order.
2. Setting of mandatory physical security 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 physical security improvements at utility facilities must be established; without sufficient funding and parallel liability exposure, pressures on utilities to minimize charges to ratepayers will take priority over physical security.

Physical Security Outlook

The near-term physical security outlook for the U.S. electric grid is fair to poor. Overall, physical security is not yet mature, well-integrated, or appropriately supported within the electric utility industry. There are significant costs to establish better physical security. Unfortunately, there are no significant operational or profit advantages to improving security practices. Some of the larger electric utilities have moved to increase physical security protections but smaller electric utilities, including municipal and cooperative utilities, often lack funding for better security. Because all utilities are electrically interconnected, a simultaneous physical attack on small utilities can cause a cascading collapse for the entire grid.

Mandatory and enforceable physical security regulation is one means of ensuring protection of the electric grid. However, without funds to improve physical security, and the opportunity to recover costs from ratepayers and/or governments, utilities will continue to resist improved protections.

Background on the Foundation Resilient Societies

The Foundation for Resilient Societies is a non-profit dedicated to the 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.

References:

1. Regalado, Antonio. "The U.S. Power Grid Remains Vulnerable to Terror Attacks." *Wall Street Journal*, August 15, 2003. Accessed March 27, 2017. https://www.wsj.com/articles/SB106090967723235200.
2. 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. https://fas.org/irp/congress/2008_hr/emp.pdf.
3. Weeks, Jennifer. "U.S. Electrical Grid Undergoes Massive Transition to Connect to Renewables." *Scientific American*, April 28, 2010. Accessed March 27, 2017. https://www.scientificamerican.com/article/what-is-the-smart-grid/.
4. U.S. Department of Energy and North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* Report. 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.
5. U.S. Department of Homeland Security. "DHS SUCCESSFULLY TESTS RAPID RECOVERY TRANSFORMERS." News release, April 2, 2012. https://www.dhs.gov/sites/default/files/publications/April%202,%202012%20DHS%20Successfully%20Tests%20Rapid%20Recovery%20Transformers_0_1.pdf.
6. National Research Council. *Terrorism and the Electric Power Delivery System*. 2012. Washington, DC: The National Academies Press. https://doi.org/10.17226/12050.
7. Smith, Rebecca. "Assault on California Power Station Raises Alarm on Potential for Terrorism." *Wall Street Journal*, February 5, 2014. Accessed March 27, 2017. https://www.wsj.com/articles/SB10001424052702304851104579359141941621778.
8. Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack." *Wall Street Journal*, March 14, 2014. Accessed March 27, 2017. https://www.wsj.com/articles/SB10001424052702304020104579433670284061220.
9. *Large Power Transformers and the U.S. Electric Grid.* Report. U.S. Department of Energy. April 2014. Accessed March 27, 2017. https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf.
10. Parfomak, Paul W. "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations." Congressional Research Service report, June 17, 2014; Washington D.C. Accessed March 27, 2017. http://digital.library.unt.edu/ark:/67531/metadc332888
11. Foundation for Resilient Societies, "Comments of the Foundation for Resilient Societies", FERC Docket No. RM14-15-000. September 8, 2014. Accessed March 27, 2017. http://resilientsocieties.org/images/RM14-15-000_Resilient_Societies_Sept_8_2014.pdf.
12. McLarty, Thomas, and Thomas Ridge. *Securing the U.S. Electric Grid*. Report. The Center for the Study of the Presidency and Congress. October 2014. Accessed March 27, 2017. https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

13. Federal Energy Regulatory Commission, "Physical Security Reliability Standard," FERC Docket No. RM14-15-000; Order No. 802. November 20, 2014. Accessed March 27, 2017. https://www.ferc.gov/whats-new/comm-meet/2014/112014/E-4.pdf.
14. "Quebec pilot accused of intentionally damaging high tension power lines." *CBC News*, June 3, 2015. Accessed March 27, 2017. http://www.cbc.ca/beta/news/canada/montreal/quebec-pilot-accused-of-intentionally-damaging-high-tension-power-lines-1.3099386.
15. U.S. Department of Energy. *United States Electricity Industry Primer.* Report. July 2015. Accessed March 27, 2017. https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf.
16. North American Electric Reliability Corporation, "CIP-014-2 — Physical Security." Reliability Standard. October 2, 2015. Accessed March 27, 2017. http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf.
17. *The State of Physical Grid Security*. Report. *Utility Dive*. 2015. Accessed March 27, 2017. http://www.utilitydive.com/library/the-state-of-physical-grid-security-2015-report/.
18. Parfomak, Paul W. "Electric Grid Physical Security: Recent Legislation." Congressional Research Service report, January 6, 2016; Washington D.C. Accessed March 27, 2017. https://fas.org/sgp/crs/homesec/IN10425.pdf
19. 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.
20. Smith, Rebecca. "Grid Attack; How America Could Go Dark." *Wall Street Journal,* July 14, 2016. Accessed March 27, 2017. https://www.wsj.com/articles/how-america-could-go-dark-1468423254.
21. 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.
22. Siemens. "Siemens mobile transformers are increasing the stability of New York's power grid." News release, March 16, 2017. Accessed March 27, 2017. http://www.siemens.com/press/en/pressrelease/?press=/en/pressrelease/2017/energymanagement/pr2017030225emen.htm&content%5b%5d=EM.