WORKING PAPER NUMBER 2017-01

Grid Security is National Security: Cyber Threats to Energy Infrastructure and Cities

Karen Weigert, Senior Fellow, Chicago Council on Global Affairs

December 2017

The lights flicker and clocks flash the wrong time. An electrical outage in the United States is often a nuisance, and typically a minor one. After a moment life, for most people, goes back to normal.

But what happens when outages aren't short-lived? The achingly slow recovery of electricity in Puerto Rico is a real time warning.

What was once a nuisance can become deadly.

In 2003 a blackout cascaded throughout the Eastern United States and parts of Canada. Over two days fifty million people lost power. The estimated impact to the United States was $10 billion in damages and 11 lives lost.

That was just two days. A blackout of a longer duration could inflict much more harm. An extended power outage would disrupt not only electricity but water, food, sanitation, health and transportation. At the extreme, a blackout has the potential to collapse the social order, threatening both livelihoods and lives.

The secret is out. In a new era of both warfare and terrorism, cyber-attacks are a growing global weapon – one that operates outside of the established Laws of War. Their frequent target is energy. According to the Department of Homeland Security energy has suffered more cyber-attacks than any other aspect of American critical infrastructure.

When it comes to defending against a cyberattack on electrical infrastructure, however, the United States is relying on a patchwork of regulations on assets that are largely privately owned.

Strong coordination between federal, regional, state, local, technical and utility organizations with standard protections and a clear delineation of roles and responsibilities is essential but currently missing. Cities, with interconnected infrastructure supporting large numbers of people, are particularly vulnerable.

Electricity anchors city infrastructure

Although electricity is national, risks will be local and often urban. Tightly interconnected critical assets in cities support many individuals in a limited geography. This increases the level of threat from an attack on energy. Cities exist just days away from chaos. The thin edge holding them together is electricity.

Electricity powers city water and sanitation systems, it allows for refrigeration of food and it powers both traffic signals and streetlights for transportation. To put it in practical terms, the potential impact to the water system alone can leave millions of people with significant health risks in a matter of days, if not sooner, from a lack of drinking water or backed up sewage. If a prolonged outage happens in winter, water in pipes can freeze causing them to burst, damaging both buildings and their contents.

At the same time, when traffic signals aren't functioning streets can quickly clog with trapped cars. At the extreme, blocked streets can prevent stores from bringing in food that residents need. The dwindling supplies that do exist will begin to rot without refrigeration. Roads that don't function also prevent residents from evacuating. The challenges, while devastating for all, are magnified for vulnerable individuals many of whom rely on electrical equipment like respirators, ventilators or home dialysis machines to stay alive.

In cities there are no silos. Increasingly the same is true for cyber-attacks.

Connected energy infrastructure expands cyber threats

Throughout decades the building blocks of the electrical system were designed to be stand-alone. Software and management systems controlled power plants and substations from the inside, in operational isolation. There were no interconnected operating systems and no internet to link to.

Today multiple existing assets are being rapidly joined through digital pathways. At the same time new assets ranging from small residential solar panels to new utility scale natural gas generation and related transmission are being brought on line. This rapid connection of old and new assets creates an "expanding attack surface" for cyber criminals.

All three aspects of the electrical system are potential targets for cyber-attacks. "Generation" of power, which typically happens in large plants located well outside of population centers, is at risk for shut down. "Transmission," which moves power long distances, getting close to the places that need it and keeping multiple parts of the United States connected and powered, is vulnerable to spreading a multi-state blackout. "Distribution," the smaller branches of the grid that deliver power to

customers, is where failure could leave specific neighborhoods, towns and cities in the dark.

Recent examples speak to the challenges – or from the attackers' point of view - to the opportunities. In late 2015 in Ukraine, hackers unleashed an attack on electricity distribution substations in the western part of the country. After months of careful planning and infiltration, they remotely took over and shut down multiple substations from three different distribution companies. Over 200,000 people plunged into darkness.

One year later Ukraine was hit again. This time a cyber-attack took out a transmission substation serving the capital, Kiev. Like the first attack, the actual blackout was short. Retroactive analysis, however, showed the operation was months in the making and even more sophisticated than the attack one year before.

Two months before Ukraine was hit for the second time, internet traffic in the United States on major sites like Twitter and Netflix was shut down. Thousands of seemingly innocuous distributed internet connected devices like home routers, cameras, even baby monitors were simultaneously taken over by a cyber-attack and redirected to flood specific systems.

This cyber-attack, known as a denial of service attack, hit small interconnected devices. These devices are similar in scope to home thermostats, small solar panels or EV charging, energy resources that are being added regularly to homes and businesses in the distribution portion of the grid, illustrating the potential vulnerability of these systems to attack.

Electricity regulation is a patchwork designed for yesterday's challenges

Energy innovation close to where people live and work isn't new. Over 100 years ago early regulation of electricity was driven by fierce competition between companies to provide power in American cities. The resulting approach generally served the needs of a growing 20th century economy; it provided economic protection for assets that were developed for the "just in time" delivery of power. But the system struggles when confronted with the 21st century challenge of cyber threats.

Cyber-attacks can hit any part of the grid making the full system part of our national defense. But the current regulatory system isn't structured to meet that reality. It isn't operationally national and it does not yet provide sufficient defense.

The majority of electrical infrastructure throughout the grid is privately held. Regulation is driven by two main regulatory bodies, FERC, the Federal Energy Regulatory Commission, and NERC, the North American Electric Reliability Corporation which extends to parts of Canada and Mexico. Regulations for new large power plants – be they solar or natural gas – as well as for the substations and transmission lines that serve them are in the FERC and NERC jurisdictions.

These regulatory structures are essentially being retrofitted in real time to incorporate cyber protection as new and existing assets are digitally joined together.

It is a colossal task, one that serves as the backbone to the provision of reliable power across the nation.

FERC and NERC cover two of the three broad aspects to the electricity system – generation and transmission of power. They exclude distribution, that last mile that brings electricity into homes and business. Distribution is where electrical assets in cities reside. It is where interconnected distributed energy resources controlled by retail customers can be found. New energy technologies can have the potential to bring great benefits to local resilience across the nation; they require a consistent security backbone as they expand.

Unlike the comprehensive structures of FERC and NERC, the regulation of energy distribution is fragmented. While utilities interact directly with the Department of Homeland Security and the Department of Energy at times, their regulation largely sits in the hands of fifty different states; each state can act independently without clear national standards.

The level of coverage and variation in approaches is significant. Few states have any policies on the books that relate to cyber threats and energy infrastructure. Current regulations broadly are also largely silent about electric utility connections with other critical infrastructure like water, leaving significant aspects of local safety without standard support.

State level regulations that do exist typically focus on utilities. Electric utilities, however, range in size and capabilities. Some operate in one city or town while others have operations across multiple states. They can be public entities or privately owned, responding to highly different goals and expectations with varied levels of financial and technical capacity.

A states-based and utilities-focused system may foster local innovation, but, without a standard baseline, it may have significant drawbacks in the realm of national security. The United States relies heavily on an inconsistent level of state regulation applied to a wide range of electrical utilities to be on the front lines in defending our communities from cyber-attacks.

This patchwork may leave vulnerabilities in many parts of the country. At the same time it may miss providing consistent protections that support local energy innovation and resilience.

Innovation is accelerating in distribution

Distributed energy technologies are scaling in cities and towns across the country. This innovation at the edge of the grid, in distribution, may be central to preventing extreme crisis.

These technologies can often withstand and recover from outages, whether an outage originates in distribution or arrives through the transmission system. Millions of urban doors have been opened to create power locally or to reduce the need for electricity coming into communities.

Solar panels can produce power on a roof, without needing to draw energy from the grid, while smart thermostats reduce the actual energy needs of buildings. Microgrids which provide power for a defined geography and can separate from the larger grid, can keep a building or a complex of multiple buildings functioning in a wider blackout. Even electric vehicle batteries can provide energy while the broader grid no longer functions.

Microgrids, which are in place in a small number of facilities, are a growing example of the energy system of the future. During Super Storm Sandy a microgrid kept the power on at Princeton University when the surrounding region went dark. Increasingly the United States military itself is deploying microgrids powered by renewables for "enhanced mission assurance."

Taking the technologies a step farther, today a solar powered microgrid is being set up in New York to allow neighbors to buy and sell renewable energy. They will do local deals using a phone app with transactions supported by blockchain technology.

While the emerging energy system is being built in fits and starts, a look ahead points to more distributed energy and more actors on the grid, transacting in a multidirectional marketplace. More devices and services offer the potential for both resilience benefits as well as points of compromise.

Future energy system security started yesterday

Addressing the energy threats of today and tomorrow requires getting ahead of the challenges, building solutions in early where possible and bolting them on retroactively where needed. The benefits of distributed energy assets must be identified and amplified. At the same time the potential risks from more open cyber portals across the grid will need to be managed.

Broad digitization and interconnectedness are reshaping the operations of the full grid. The Electricity Information Sharing and Analysis Center (E-ISAC) is a division of NERC that partners directly with industry on threats and vulnerabilities of all kinds. Its strategic plan identified a risk from technology that in the 5-10 year horizon the ability to run core aspects of the grid manually "might be lost."

Today in multiple locations around the country electricity customers no longer just consume power. Users are now producers. In a multidirectional marketplace, customers also provide grid services. The enabling technologies and procedures for the emerging energy marketplace are not yet built – and neither is the foundation for cyber security.

Cyber protections will need to be effective in a future energy system that may look as much like the financial sector, with multiple entities creating and transacting, as it does traditional infrastructure.

Building from today

From generation through transmission and into distribution, the grid is becoming more complex and interconnected. At the same time cyber-attacks are growing in focus and capability. In the middle of these transitions sit the communities we call home.

Today this threat to national security is not matched with an adequate national response. There is no jurisdictional owner to address preventing and recovering from cyber-attacks. A stronger focus on cyber threats and energy infrastructure for cities is needed.

Here are four places to start:

1. Augment the foundation of cyber protection in the core grid

In an era of evolving threats, the fundamental protections in the generation and transmission systems must be strengthened. FERC and NERC, with specific protocols for Critical Infrastructure Protection (NERC CIP), have moved to incorporate cyber threats into their structure. NERC recently held its biennial grid security exercise, GridEx, to simulate cyber/physical attacks and test the full ability of utilities and partners to respond.

For those who opt in, GridEx serves as a flexible testing ground. Cyber threats are volatile, never static. Many mandatory approaches, however, are based on specific thresholds, similar to tree trimming requirements in the physical world. A rapid evolution that leverages approaches anchored in threats and objectives, essentially capability driven, could help address gaps. A seemingly old-school approach may also be required, manual controls so that infrastructure can be restarted in a severe crisis.

Platforms like E-ISAC serve as bridges and, increasingly, strategic partners. Closer alignment between threat identification and industry is critical. One of the leading drivers of corporate investment in cyber security technology is addressing regulation. Processes which raise the importance of a relevant and consistent approach from core partners is needed to both unlock spending and focus it well.

2. Strengthen baseline protections against national threats with roots in distribution

National threats do not reside on only one side of the transmission - distribution line. The blackout of a large city is a case in point.

Fifty separate state approaches are unlikely to deliver a uniform level of national security from cyber-attacks. Growing technologies like microgrids, which can offer significant protections, are being built without clear cyber-security protocols. Consistent cyber standards in hardware and software in grid connected assets can help protect cities and communities.

In a world of increasing connections, multiple sectors will need to be engaged to manage threats. In particular a platform that allows state-based public utility commissions (PUCs) nationally to both engage in the discussion and to consistently implement best practices will be critical; this could also help in addressing the staffing pressure at the state level where PUCs cover a wide range of issues. Developers of new grid connected technologies will also need to be engaged. Utilities that operate across state boundaries have a unique role to play, particularly if they can effectively partner with multiple PUCs.

3. Demonstrate and reward the benefits of resilience today

A grid attack that impacts the actual delivery of energy in the United State may still happen. GridEx is a critical start in ensuring that the potential damage is minimized. It needs to be married to a robust plan that strengthens operations and expands resilient infrastructure.

The basics of network segmentation, backup and restore procedures, and robust training for staff that will be bringing the grid back up in a crisis must be strongly rooted across organizations. At the same time distributed energy solutions diversify the number and types of critical nodes supporting electricity in an urban center. This diversity in energy resources should increase the complexity in executing a cyber-attack, making it much harder to cause a city-wide blackout and much more challenging to sustain one.

First and foremost, these benefits need to be clearly demonstrated with metrics that are anchored in data from current and new installations. Second, this value needs to flow through the regulatory and management oversight of the grid. PUCs often determine the financial structures that support local energy resources. In addition, ten RTOs and ISOs, Regional Transmission Organizations and Independent System Operators, manage grid operations in wholesale markets across all fifty states. The potential resilience benefits of distributed energy resources typically aren't valued in the state-level Renewable Portfolio Standards and Energy Efficiency Portfolio Standards that direct the flow of local energy resources, and are also not yet broadly recognized in wholesale markets. They will need to be if the protections from distributed asset are to be scaled.

With the increased clarity on the benefits from distributed energy, local asset owners – from private locations through cities – can identify critical nodes and prioritize local energy resilience.

4. Invest in the cyber foundation of the future energy marketplace

The energy system is evolving rapidly yet the specific guidelines, protocols and regulations of the future remain largely undefined. What is clear is that the national electricity system is becoming increasingly digital, interconnected and distributed. Overall these transitions offer new benefits to the grid. Potential future cyber regulation or oversight should not stand in the way of new grid innovation. Increasingly, however, digital, interconnected and distributed assets stress the

system today and point to the need for cross sector engagement and consistent cyber standards now.

A collaboration platform that involves federal and state regulators, the energy industry and city leaders must be created to inform both regulation and industry best practice. Its ranks must also be filled with cyber experts from the financial, engineering and education sectors as energy takes on more virtual and financial characteristics. As a foundational element, the Unites States is under-represented in cyber expertise. This growing sector with nationwide job creation potential merits further investment.

Insurance policies generally do not yet address the linked threats of cyber and will need to respond to residents. Ultimately, in the face of disaster recovery, FEMA may need to provide support; the protocols to assist residents recovering from devastation stemming from a well-executed cyber-attack are largely missing today.

Conclusion

The United States electricity system has long been at the forefront of both societal benefit and innovation. Electricity served as the foundation for the expansion and prowess of the United States economy in the 20th century, and national investments cultivated once early-stage technologies like solar panels and wind turbines that are currently scaling the globe.

In a rapidly changing world, bold steps are again needed. Early electricity regulation grew out of the needs of cities, and yet today, cities lie in the least standardized part of the grid. To build the foundation of a thriving economy, reliable, resilient and clean energy must be available.

Today, however, there is no coordinated and integrated national forum addressing cyber threats to energy infrastructure and cities nor a platform to enable the grid edge resources that may offer unique local protections.

A cyber-attack has not yet thrown American cities into prolonged darkness. A concerted effort is needed to keep it that way.

This paper was informed by off the record conversations conducted with experts from multiple sectors including government, industry and nonprofit organizations.

To provide comments or input please reach out to kweigert@thechicagocouncil.org

Karen Weigert is a senior fellow on global cities at the Chicago Council on Global Affairs. She served as the first Chief Sustainability Officer of the City of Chicago from 2011 to 2016 and is on twitter @KarenRWeigert.