MI

June 2016

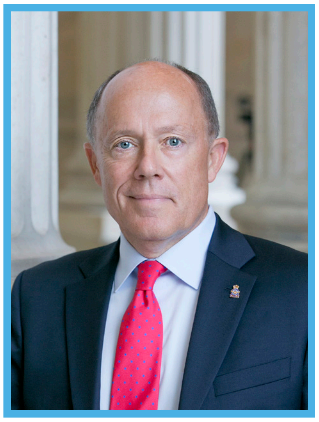
REPORT

EXPOSED

HOW AMERICA'S ELECTRIC GRIDS ARE BECOMING GREENER, SMARTER—AND MORE VULNERABLE

Mark P. Mills
Senior Fellow

About the Author



Mark P. Mills is a senior fellow at the Manhattan Institute, CEO of the Digital Power Group (a tech-centric capital advisory group), faculty fellow at Northwestern's McCormick School of Engineering and Applied Science, and an advisory board member of Notre Dame University's Reilly Center for Science, Technology, and Values. Previously, he cofounded and was chief tech strategist of Digital Power Capital, a boutique venture fund, and was chairman and CTO of ICx Technologies, helping take it public in 2007. Mills is a contributor to Forbes.com and coauthor of *The Bottomless Well: The Twilight of Fuel, the Virtue of Waste, and Why We Will Never Run Out of Energy* (2005). His articles have been published in the *Wall Street Journal* and *New York Times Magazine*.

Earlier, Mills was a technology advisor for Bank of America Securities and coauthor of the *Huber-Mills Digital Power Report*, an energy-tech investment newsletter. He has testified before Congress and has briefed many state public-service commissions and legislators. Mills served in the White House Science Office under President Reagan and subsequently provided science and technology policy counsel to numerous private-sector firms, the Department of Energy, and U.S. research laboratories.

Early in his career, Mills was an experimental physicist and development engineer at Bell Northern Research (Canada's Bell Labs) and the RCA David Sarnoff Research Center on microprocessors, fiber optics, missile guidance, nuclear energy, and nonproliferation, earning several patents for his work. He holds a degree in physics from Queen's University in Ontario, Canada.

Contents

Executive Summary

Electric grids have always been vulnerable to natural hazards and malicious physical attacks. Now the U.S. faces a new risk—cyberattacks—that could threaten public safety and greatly disrupt daily life.

Utility executives and other experts argue persuasively that U.S. grids, especially long-distance grids, are currently well secured. Yet the key issue is not today's security but tomorrow's. Here the risks are growing rapidly. The push for "greener" and "smarter" grids requires far greater grid-Internet connectivity to ensure the continuous delivery of electricity. These greener, smarter grids will involve a vast expansion of the Internet of Things that greatly increases the cyberattack surface available to malicious hackers and hostile nation-state entities.

Cyberattacks overall have been rising 60 percent annually for the past half-dozen years, and utilities are increasingly targeted. A Cisco study found that 70 percent of utility-security professionals say that they have experienced at least one security breach. For their part, federal and state governments genuflect to the goal of reliable, resilient, and affordable electric service. Yet comparatively trivial sums are directed at ensuring that grids are more secure, compared with the vast funding to promote, subsidize, and deploy green energy on grids.

The central challenge for U.S. utilities in the twenty-first century is to accommodate the conflict between political demands for more green energy and society's demand for more reliable delivery of electricity. Greater grid cybersecurity in the future means that policymakers must rethink the deployment of green and smart grids until there are assurances that security technologies have caught up. While the government needs to improve its vital role in helping with cyber "situational awareness," the private sector must lead the way in defending against cyberphysical threats that evolve and move at tech-sector—not bureaucratic—velocities.

To lay out the state of affairs and provide recommendations for sensible U.S. grid cybersecurity policies, this report examines:

1. The forces that have made electricity far more critical than ever. The "information economy" is fundamentally electricity-dependent and is now a threefold bigger part of U.S. GDP than the oil-dependent transportation sector that dominated America's economy in the twentieth century.

2. The structure of America's grids and the history of blackouts. Outages have become increasingly common. Lloyd's estimates that the damage from worst-case outage scenarios from cyberattacks would range from nearly $250 billion to $1 trillion.

3. The challenge of an "on-demand" economy that is escalating the peak demands for power. The twenty-first century's unique—and widening—gap between average and peak energy demand is forecast to more than double in the coming decade, even as far more episodically available green-generating capacity is added to the grid.

4. The new character and magnitude of cyberphysical threats. A recent report found an over 400 percent rise in 2015 in the number of times that hackers probed for vulnerabilities in cyberphysical systems, a.k.a. the "Internet of Things." With security experts claiming that the "next Cold War has already begun—in cyberspace," the key is to keep critical infrastructures, especially electricity, off the front lines.

5. The skewed priorities in grid spending. During the past decade, wind and solar power, which cannot meet society's 24/7 energy needs, accounted for over 75 percent of new generating capacity. In the same period, more than $150 billion in federal spending went to green- and smart-grid programs, while the U.S. Department of Energy spent $150 million on cybersecurity R&D.

6. The state of grid cybersecurity today. Even as cybersecurity concerns are causing most other industries to integrate cautiously into the Internet of Things, policymakers—despite warnings from the U.S. Department of Homeland Security—are pressing electric utilities to accelerate grid integration with the Internet.

EXPOSED

HOW AMERICA'S ELECTRIC GRIDS ARE BECOMING GREENER, SMARTER— AND MORE VULNERABLE

I. Introduction

Nearly everyone is aware of the deep interconnectedness of electricity in every facet of daily life. Less well understood is the enormous size and complexity of America's roughly $6 trillion electric utility system.[1] Unlike in many countries, the U.S. electric utility system is *not* a single grid. Rather, it is a complex web of eight regional "supergrids" coupled with thousands of local grids that deliver 55 percent of all the energy that America uses for non-transportation purposes.[2] Now, the U.S. electric utility system is on track to deliver an increasing share of the country's transportation energy, too.[3]

The August 2003 blackout that enveloped New York City and the Northeast—which put 50 million people in the dark for two days—inflicted $6 billion in damages.[4] That outage was caused by a confluence of human and machine factors, as are so many disasters in complex systems. Nature, thus far, is the most common source of grid outages. In 2005, Hurricane Katrina left nearly 3 million without power for several days.[5] In 2011, it was the lingering power blackouts that amplified the impacts from Hurricane Sandy—accounting for some 40 percent of the $50 billion in damages from that storm.[6]

The second most dramatic takeaway from widespread outages—after their economic and social costs—are the heroic efforts and speed with which electric utility crews effect repairs and restoration.[7] Utilities have long prepared for recovery: geographically widespread, complex systems have unavoidable exposure to natural events and statistical failure modes. In the wake of the 2003 blackout, a Carnegie Mellon University study estimated that a blackout of that level is likely every 25 years.[8] In the meantime, smaller but still inconvenient outages—resulting from nature as well as other causes—are becoming more common.[9]

But America’s electric sector faces two revolutionary changes. One is the emergence of so-called smart systems that promise vastly improved control and distribution of power across grid systems. The other is the pressure to add far more episodic (wind and solar) power sources that inherently require “smart systems” linked to the Internet.

Information and communications technologies (ICT) are now migrating from working mainly with information (i.e., the cyberworld) to an Internet of Things (IoT) that can also act directly in the physical world. This “cyberphysical” transformation holds the potential for greater efficiencies, convenience, reliability, safety, and predictability. For example, information systems are already very good at identifying and predicting road traffic and hazards, as well as informing drivers via maps and alerts. When that information is converted into a direct action as a cyberphysical system, one gets an “autonomous” (i.e., driverless) car.

Cyberphysical systems, however, bring a new class of risk; let’s call it “cyber carjacking.” In the summer of 2015, hackers remotely took over the steering and braking of a Jeep Cherokee (**Figure 1**).[10] That wake-up episode led to a 1.4 million vehicle recall by Chrysler.[11]

Figure 1. Anatomy of a Cyberphysical Hack

In 2015, researchers Charlie Miller and Chris Valasek took control of a Jeep from ten miles away.[12] The engineers looked for a vulnerability in Sprint’s cellular network that connected to the vehicle’s music and radio system, and then hacked the password. Next, exploiting the fact that a Jeep’s entertainment system is physically connected to the power system, they remotely uploaded new code onto the car’s microcomputers (all on the same power network) that controlled steering and antilock brakes. Chrysler and the cellular carrier have since corrected those particular vulnerabilities; but cyberphysical systems remain complex, diverse, and rapidly evolving.

The challenge for electric grids across America comes from the push for greener, smarter grids, wherein all such technologies demand real-time controls and Internet connections. Smart appliances, solar arrays, battery-storage, and demand-management technologies require the kind of computer-based controls—the equivalent to automotive antilock brakes and power steering—to manage the episodic, varied nature of power demand and supply on grids required to meet society’s 24x7 needs. Engineers and cyber experts have understood for years the nature of such exposure.[13] But now, the proliferation of real-time networked controls on grids will vastly increase the variety and scale of the cyberattack surface.

For aircraft and cars, safety and security take priority over the efficiency and convenience gains from using automated and networked controls. Not so for U.S. power grids, where cyberphysical security has taken a backseat to policymakers’ push for green-energy priorities. Even when cybersecurity is on the political front burner, the utility sector is frequently omitted. The president’s new Commission on Enhancing National Cybersecurity, for instance, includes no appointees from the infrastructure and electric sectors.[14]

In pursuit of environmental aims, U.S. policymakers and regulators are rushing to improve energy efficiency and integrate episodic power sources—i.e., wind and solar—onto electric grids. This has involved pushing utilities and federal and state governments to spend tens of billions of dollars on smart-grid technologies. For everything from cars to aircraft to health care, regulators have emphasized a safety-first approach to technology. That has not been the case thus far with regard to ensuring the cybersecurity of America’s evolving electric grid.

This head-in-the-sand attitude may be slowly changing. The December 2015 hacker-caused blackout of Ukraine's electric grid helped raise red flags, as did the discovery that, in 2016, Iranian hackers used a process called "Google dorking" to hack into a small New York dam's control system.[15] The Ukraine hack, ostensibly by Russia, used malware called "BlackEnergy" combined with other cyber and espionage tactics. Arguably the first wake-up call regarding the capabilities of cyberphysical attacks came in 2010, when the world learned of a clandestine project (ostensibly U.S.-Israeli) using the Stuxnet computer virus to severely damage the electrical infrastructure of Iran's nuclear facilities.[16]

Last year, Lloyds Bank published a comprehensive study of worst-case scenarios "to bring awareness to the potential physical damage caused by cyberattacks against Operational Technology" and, in particular, "the U.S. power grid." Lloyds noted that, while the scenarios considered were still "improbable," they were nonetheless "technologically possible."[17] A worst-case multipronged, multiregional cyberattack causing widespread outages could inflict $243 billion–$1 trillion in total damage on the U.S. economy, Lloyds found.

Current electricity policies, as will be discussed in greater detail below, run the risk of creating the conditions for a perfect cyberstorm by prematurely pushing the Internet of Things onto grids to accommodate environmental goals—and doing so at a time of growing cyber capabilities of bad actors, and exactly when society is becoming increasingly dependent on electricity.

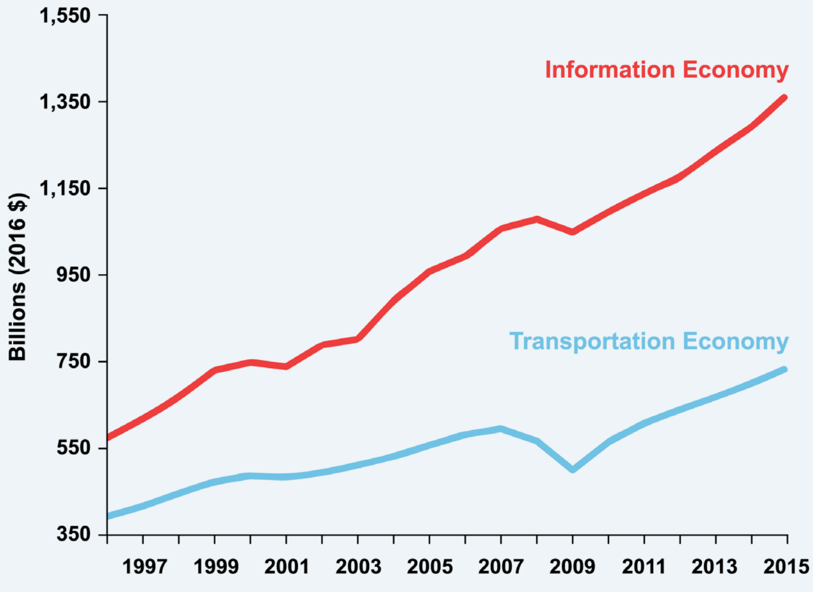
II. The U.S. Is Increasingly Dependent on Electricity

Individual data centers—the central power plants of the Internet—consume as much power as steel mills.[18] Yet only several decades ago, data centers did not exist as a category for tracking electricity use.[19] Even more than factories, data centers must run 24/7. And while data centers—enormous information "factories"—today consume more U.S. electricity than America's steel industry, they account for only a fraction of the information ecosystem's total power needs.[20]

Overall, the U.S. economy is more dependent on the information-centric and electric-dependent sector than the transportation-centric, oil-dependent sector that dominated the twentieth century: activities associated with transporting goods and people account for about $500 billion of U.S. GDP; the comparable figure for creating and transporting information is $1.2 trillion (**Figure 2**).[21]

FIGURE 2.

U.S. GDP Associated with America's Transportation and Information Sectors



Data Source: U.S. Bureau of Economic Analysis[22]

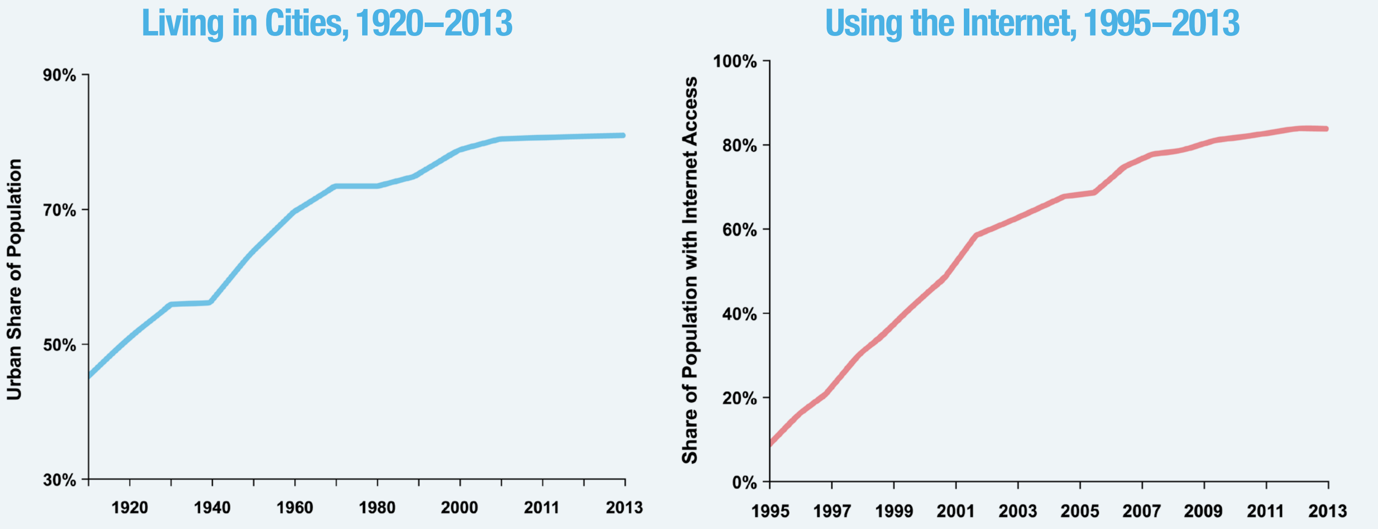
This dependence on electricity-using data networks is growing. Cisco Systems, a maker of computer-networking devices, forecasts U.S. data-center traffic to nearly triple in five years, with much of that growth coming from the explosion of video content.[23] Cisco also projects a tenfold rise in data traffic from the Internet of Things, including from machines in homes, cars, stores, factories, hospitals, and, especially, utilities.[24] By one estimate, global IoT data traffic could require as many as 4,000 new data centers, creating an aggregate power demand fourfold that of California's grid.[25] Many of those data centers will be in America. While information hardware will continue to become more efficient, overall ICT power demands will continue to grow.[26]

Then there are other electricity-consuming tech trends, including 3-D printing, data-centric health care, and electric vehicles (EVs). The U.S. Energy Information Administration's (EIA) forecast for EVs on U.S. roads by 2030 represents adding the electric-load equivalent of 5 million homes.[27] Other, more ambitious, EV forecasts add demand equivalent to 40 million homes.[28]

Rising urbanization—in the U.S. and globally—deepens electric dependency, too. Cities, inherently highly electrified (**Figure 3**), will see accelerated dependence with the "smart city" movement, wherein everything from traffic to building operations to public services and safety are Internet-connected.

While energy efficiency is projected to improve, the EIA forecasts that America will use about 10 percent more electricity two decades from now.[30] Over the same period, the EIA forecasts essentially no growth in U.S. transportation oil demand. These two trends mean that the U.S. economy will become yet more dependent on fuel delivered by the kilowatt-hour in wires, not by the gallon in pipes. The big challenge remains: to ensure that this electricity reaches our homes, hospitals, and businesses whenever we need it.

FIGURE 3. **Share of U.S. Population…**



Living in Cities, 1920–2013

Using the Internet, 1995–2013

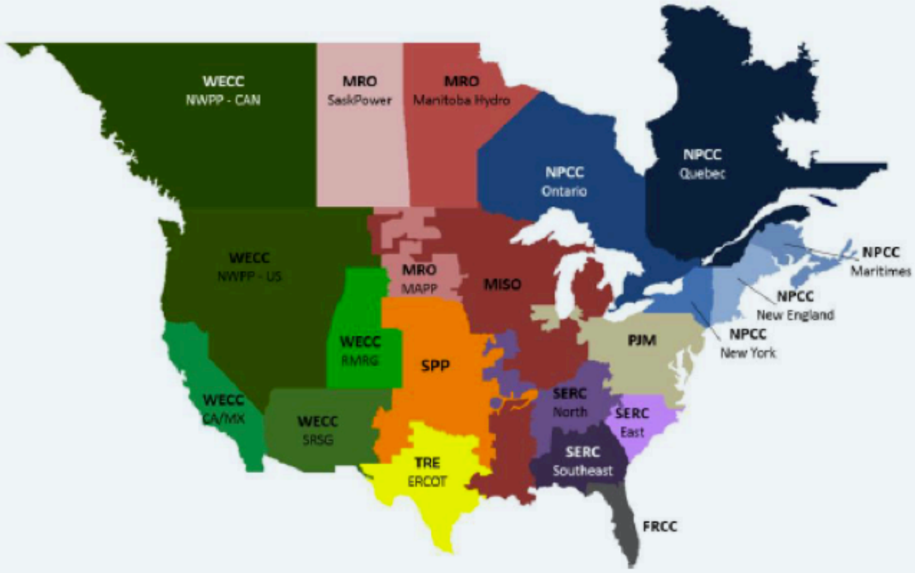
Source: Kleiner Perkins Caufield & Byers[29]

III. The Electricity Balancing Act

Unlike many other countries, the U.S. does not have a national electric grid. Instead, it has a complex array of grids, a "system of systems." There are two classes of U.S. grids, as well as many separate individual grids within them. One class consists of North America's eight long-haul grids, Regional Transmission Operators,[31] which move "bulk power" from remote power plants to cities, each of which has regional subdivisions (**Figure 4**). The long-haul grids are overseen by the North American Electric Reliability Corporation (NERC) and are regulated by the Federal Energy Regulatory Commission (FERC).

FIGURE 4.

America's Eight Long-Haul Transmission Grids



Source: NERC

The second class of U.S. grids includes thousands of independent local distribution grids, from small towns to the biggest metropolises. These grids are owned, or used by, more than 3,000 utilities. About 200 of the utilities are investor-owned, about 900 are rural cooperatives, and about 2,000 are publicly owned municipal entities.

With every other commodity's supply chain—including oil, natural gas, minerals, and agricultural products—there are typically one to several months' worth of demand in storage to ensure reliable delivery to markets. Given the physics of storing power, however, 99 percent of electricity has to be generated the same instant that it is consumed.

Today's central engineering challenge is to deliver power continuously—and nearly instantaneously—over vast geographic areas in the face of inevitable plant failures, weather, and fluctuating demand.

The invisible balancing act needed to keep huge power flows stable can be loosely analogized to trying to run with a shallow pan full of water without spillage. If grids are not balanced continuously, critical voltage or frequency control can be lost, leading to outages, damaged customer and utility equipment, and, in some cases, the destruction of grid hardware. To counter such risks, grids have long been fitted with sensors, protective relays, backup systems, safeguards, and manual overrides, as well as with various supervisory control and data acquisition systems (a kind of precursor industrial "internet" used in nearly all industries and infrastructures).

Ultimately, technology will permit America's electric grids to operate in a fashion more akin to the Internet: one day, the grid will be nodal, interactive, and highly controllable, with smart power-flow routing, micro-grids, solar energy, and batteries all playing a role.

Next-generation high-power semiconductor technologies are emerging to make grid-level dynamic switching and control possible; but such technologies will take time to deploy and to ensure that they are cybersecure. Still, when such power control becomes widespread, the primary benefits will extend beyond enabling more EVs and solar on grids. Above all, the benefits will involve enabling better security and reliability.

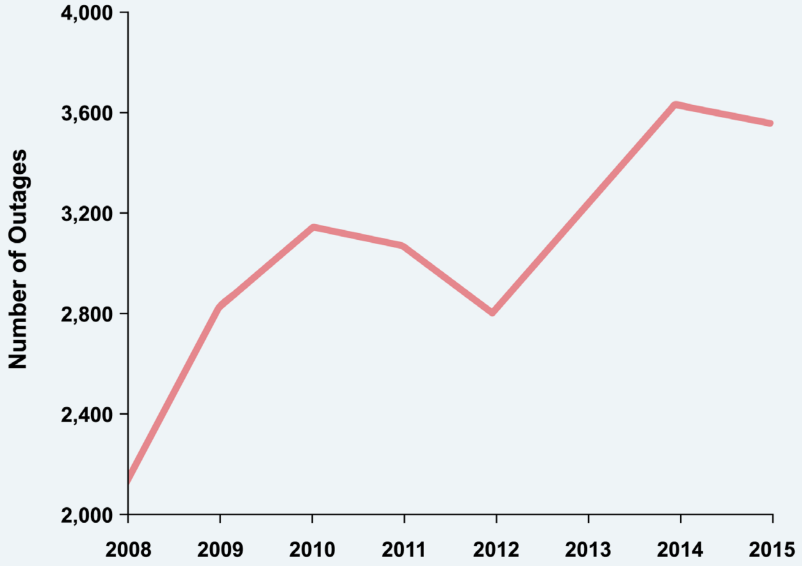
To date, however, spending to make the grid smarter has been dominated by making it easier for utilities to bill customers, or promote conservation and green energy.[32] Adding communications features to meters is comparable to installing a speedometer or gas gauge—it is not a game-changer. The game-changer involves controlling grid-power flows and doing so securely.

IV. Blackouts: Past, Present, and Future

Electric power outages are becoming more frequent (**Figure 5** and **Figure 6**). Since 1990, the average incidence of outages on U.S. grids has increased by about 8 percent per year,[33] while the annual outage duration has risen by about 14 percent per year.[34]

FIGURE 5.

U.S. Electric Power Outages

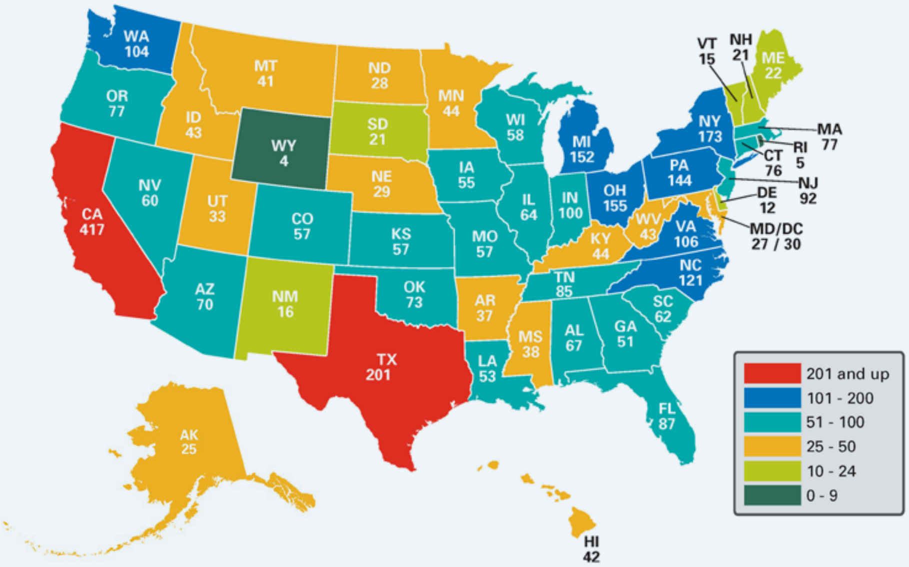


Data Source: Eaton Blackout Tracker

The social disruption—not to mention the costs—wrought by blackouts is substantial. (**Figure 7**). Consider New York City, which, on August 31, 1959, was struck by the world's first major electric-power outage. Triggered by a heat wave and surging air-conditioning use, the outage wiped out power across 500 blocks of Manhattan for 13 hours.[35] On November 9, 1965, 30 million people in the Northeast, including millions of New Yorkers, were plunged into darkness for 18 hours. That blackout inspired books and movies, mostly about heroic behavior and rediscovered neighborliness, and led to the creation of NERC, which established standards and oversight to improve long-haul grid reliability.

FIGURE 6.

Power Outages in 2015 by State



Data Source: Eaton Blackout Tracker

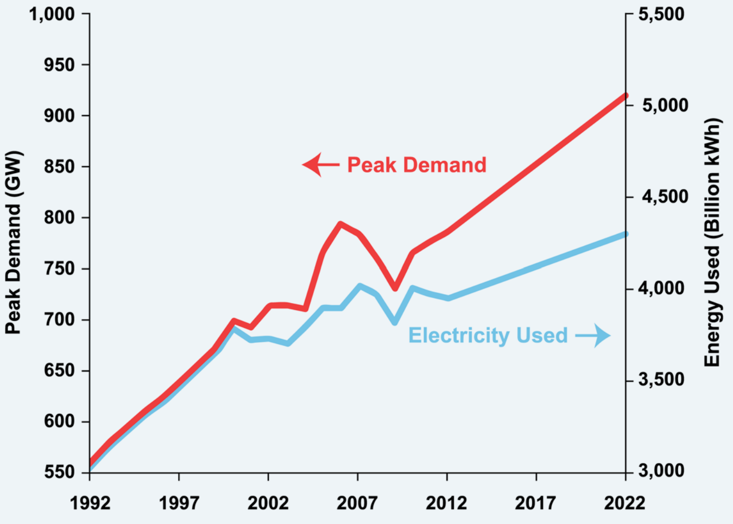
Figure 7. America's Ten Worst Blackouts[36]

1. **August 14, 2003:** 50 million people lose power across the Northeast
2. **November 9, 1965:** 30 million lose power across the Northeast and in Ontario, Canada
3. **July 13, 1977:** 9 million lose power in New York City
4. **October 22, 2012:** 8 million lose power across the Northeast
5. **August 10, 1996:** 7 million lose power across the West
6. **December 22, 1982:** 5 million lose power across the West
7. **June 29, 2012:** 4 million lose power across the Midwest and the Northeast
8. **October 29, 2011:** 3 million lose power across the Northeast
9. **September 8, 2011:** 3 million lose power in California and Arizona
10. **July 2, 1996:** 2 million lose power across the western U.S., Canada, and Mexico

New York City's most infamous blackout struck on July 13, 1977.[37] The outage lasted 25 hours and sparked mass looting and arson—1,600 stores were ransacked, and more than 1,000 fires were lit[38]—prompting more than 4,000 arrests and headlines such as "Night of Terror."[39] The total damage was estimated at $300 million. New York City has since suffered three more blackouts, all a product of nature and machine/human failure.

FIGURE 8.

U.S. Electricity Energy Consumption v. Peak Power Demand



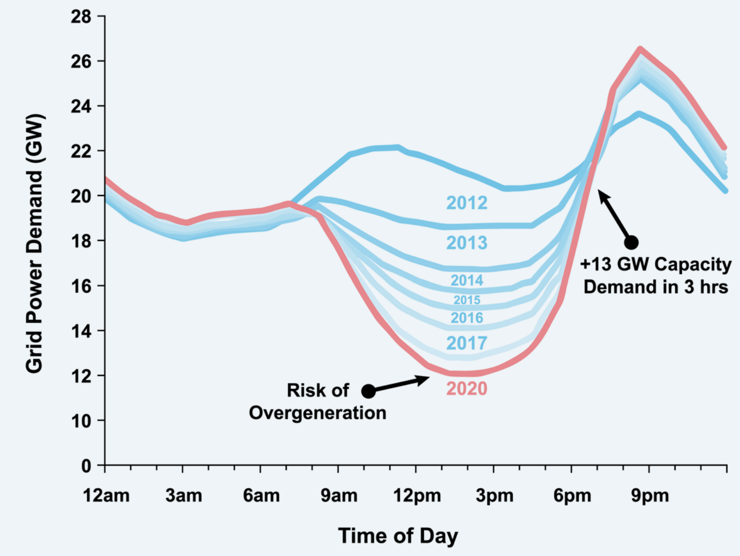
Data Source: Electric Power Research Institute and EIA

Today, all major cities use far more electricity than New York City consumed on the eve of its disastrous 1977 blackout. Meanwhile, a new phenomenon has emerged for utilities, with important implications for reliability: peak demand for power has become far more volatile.

For more than a decade, there has been a widening gap between the growth rate in energy used to make electricity and the growth rate in peak demand (**Figure 8**).[40] As a result, an increasing share of standby generating capacity is required to meet frequent, episodic peaks. This also means that for many utilities, as much as 70 percent of total costs are associated with capital equipment (power plants, wires,

FIGURE 9.

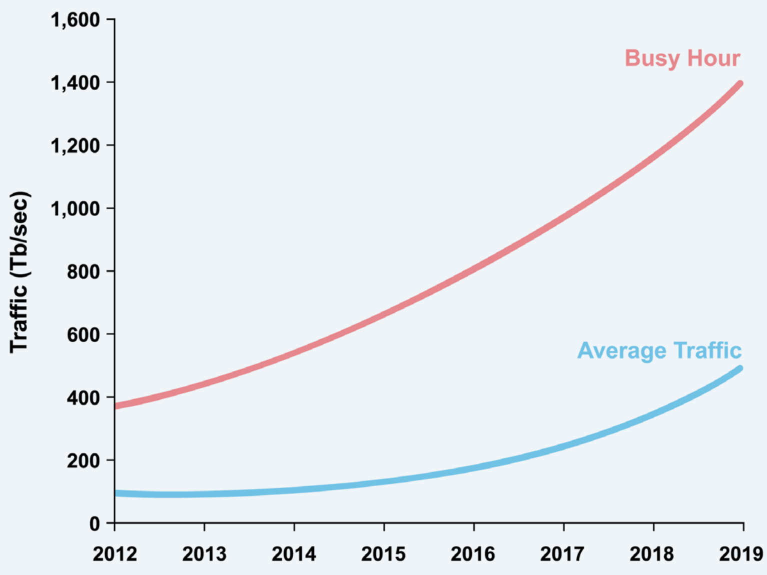
Daily Variation in Electricity Demand, California Grid



Source: California ISO

FIGURE 10.

Peak v. Average Global Data Traffic



Data Source: Cisco[45]

hardware) to ensure peak-delivery capacity. These costs and hardware are essentially independent of how much energy is consumed. Put another way: reliability is determined more by the amount of capital spent on hardware to ensure that energy is available when needed, rather than on the money spent producing the energy itself.

This trend is visible across America, including New York City.[41] Official forecasts expect little growth in New York City's average utility energy consumption; but *peak* demand is expected to rise sharply, from 160 percent above average demand in 2003 to 220 percent above average demand in the next decade.[42]

The challenge of dealing with increasing disparity between peak and average *demand* will be radically exacerbated with the addition of more episodic, or peak, *supply* from solar and wind. This new challenge is particularly clear when viewed on an hourly basis in California, where the rapid growth in green energy will cause the daily peak-to-valley ratio to rise from 115 percent in 2012 (i.e., meeting peak demand required 115 percent of base generation) to about 145 percent in 2020 (**Figure 9**). As the California ISO, the state's transmission authority, notes, this will "require flexible resource capabilities to ensure green grid reliability."[43]

America's "information utilities" (i.e., data centers) are also seeing surging peak demand. According to Cisco, the gap between peak data traffic and average data traffic (visible in its tracking of global data use) will widen hugely in the coming decade, from 200 percent today to nearly 700 percent within a few years (**Figure 10**).[44]

There are two main tools to manage peak demand of anything: build extra capacity, or incentivize customers to consume less during peak times. Information utilities use the former, furiously expanding infrastructure to meet demand. Electric utilities—prodded by regulators—prefer the latter, harnessing technology and price incentives to moderate peak demand.

Peak electricity-management techniques require substantially increasing communications and controls. In other words, they require a far greater expansion of the Internet of Things onto local grids.[46] The majority of products forecast for the growing residential IoT sector are associated with controlling electricity by integrating information controls—i.e., adding "smart"—into meters, thermostats, air conditioners, heaters, lights, PV systems, batteries, and EV chargers.[47]

Without a more widely networked, IoT-centric electric grid, meeting peak demands, ensuring reliability, and, as discussed later, fuller deployment of solar and wind sources will be impossible. The current rush to push the Internet of Things onto the electric grid will dramatically raise the risks of cyberattacks. Asked for his view of the Internet of Things, Jerry Irvine, a cybersecurity expert, responded: "Scary as hell."[48]

V. Grid 2.0: A Cyberphysical Target for Hackers

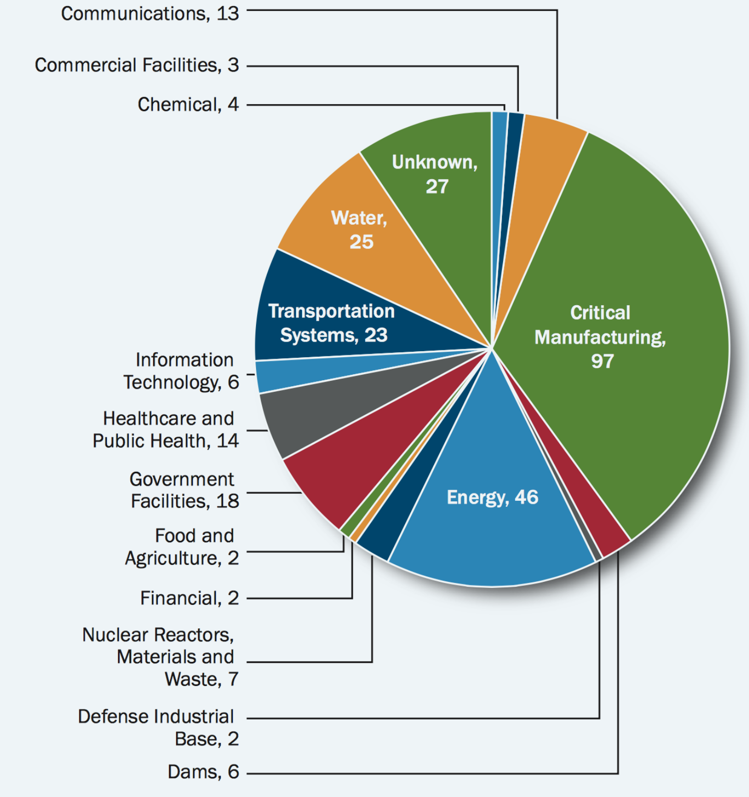
There are two main types of cyber targets: cyber information targets and cyberphysical targets. The vast majority of cyberattacks fall into the former, which includes theft of financial and other personal information, theft of business secrets, and harassment, such as "distributed denial of service," or DDoS, attacks to overwhelm and shut down websites.

But cyberphysical targets are becoming more vulnerable and more attractive to bad actors.[49] In 2000, in the first known example of a malicious breach into an industrial control system, an angry ex-employee hacked an Australian water-services plant and released tons of sewage into local parks and rivers.[50] In 2003, after a consultant inadvertently bypassed a firewall, Ohio's Davis-Besse nuclear plant's control room was infected by the Slammer cyberworm, which then blocked the plant's automated sensors.[51]

Still more recently, in 2012, hackers wiped out the hard drives on 35,000 Saudi Aramco computers, temporarily compromising all back-office operations of the state-backed oil giant. Shortly before the 2014 Winter Olympics, a hacker gained access to the heating, cooling, and emergency-response systems of Russia's Sochi arena.[52] In 2015, German engineers discovered that hackers had breached the operating system of a steel mill, causing "massive physical damage."[53] In America, cyberterrorists are broadening their reach

FIGURE 11.

U.S. Targets of Cyberphysical Attacks by Industry, 2015



Source: National Cybersecurity and Communications Integration Center[59] beyond their traditional financial and personal-information targets to include the power systems and the machines inside hospitals. Their goal: "Bring these hospitals to a standstill."[54]

Measuring the precise number of attacks on cyberphysical systems is not easy, since there are many standards and definitions. But the reported trends are clear: hackers are increasingly targeting infrastructure systems.

According to computer firm CDW, in 2015, the number of cybersecurity attacks at U.S. utilities exceeded 7,000. America's oil and gas sector experienced more than 5,000 attacks.[55] According to Tripwire, an IT security firm, 75 percent of utilities report that at least one cyberattack defeated their firewalls and antivirus programs in 2015, and 80 percent worry that a future attack could cause physical damage.[56] PwC, an auditor, reports that cyberattacks on the U.S. utility sector perpetrated by organized crime doubled in 2015.[57] According to the federal National Cybersecurity and Communications Integration Center, America's manufacturing and energy sectors are the top two targets for attacks on cyberphysical systems (**Figure 11**).[58]

In another study, Cisco found that over 70 percent of utility IT security professionals discovered a security breach in 2015, compared with 55 percent in other industries.[60] U.S. utilities were among the top five most exposed American industries to malware, says Cisco.[61] Some security experts even warn that the "next Cold War has already begun—in cyberspace."[62]

To win this new cyber war, America must keep electricity and other critical infrastructure off the front lines. Alas, simply detecting attacks can be difficult. The SANS Institute, a cybersecurity research outfit, says that, when it comes to the Internet of Things, "it's almost impossible to tell how often" industrial controls are breached or "how it's done."[63] According to Tripwire, only 43 percent of energy executives believe that their firms have detected all cyberattacks committed against them.[64] AT&T says that, in 2015, there was a 458 percent increase in the frequency with which hackers probed IoT connections for vulnerabilities.[65]

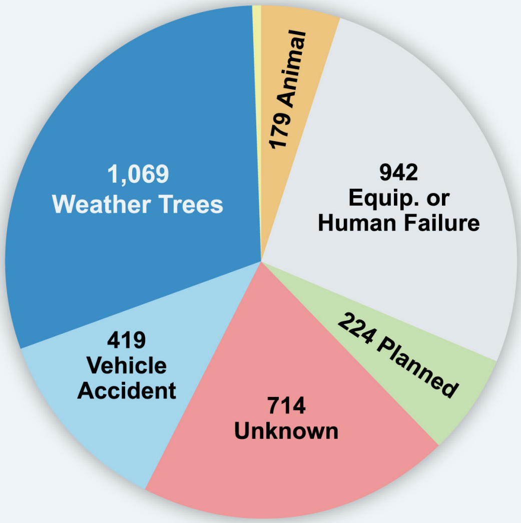
Where are the vulnerabilities? Utility smart meters, one of the most prominent ways that the Internet can be connected to the electric grid, are one. Since 2010, the number of smart meters in the U.S. has soared, from 10 million to more than 50 million.[66] But in the years to come, smart meters will represent only the tip of the iceberg of vulnerabilities in an expanding attack surface of IoT-enabled devices connected to grids.

The proliferation of Internet-connected things with direct access (or back doors) to electric grids is not the only threat to their security and reliability; so, too, is the push to accelerate a fully cyber-connected electric grid. Meanwhile, the SANS Institute reports that only 29 percent of U.S. companies are beginning to implement a cyberphysical strategy, 33 percent are still developing a strategy, and 18 percent have no plans to develop a strategy.[67]

There are yet no documented cases of terrorist attacks triggering U.S. power outages. Still, it is possible that cyberattacks may be to blame for some outages that have been categorized as "faulty equipment" or "unknown" causes (**Figure 12**). It is a near-certainty, however, that "cyberattack" will soon become a new category for power-outage tracking.

FIGURE 12.

Causes of Reported U.S. Grid Outages, 2015



Source: Eaton Blackout Tracker

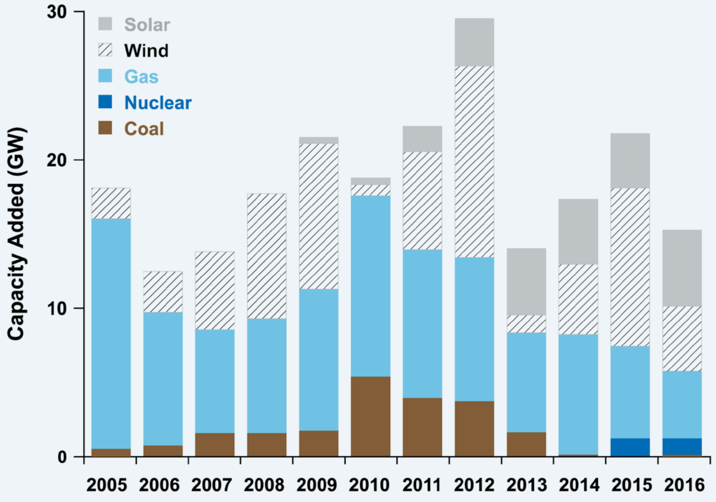
VI. Green Energy v. Cybersecurity

State and federal mandates (including the federal Clean Power Plan) seek to move U.S. electricity generation away from fossil fuels and toward renewable power sources. Total federal and state support for green-energy tech over the past decade exceeded $175 billion.[68] By comparison, over the past half-dozen years, the DOE invested a total of only about $150 million on cybersecurity research projects.[69] The risks inherent in this asymmetry are not only associated with a lack of emphasis on cybersecurity; they also involve the structural changes being brought to U.S. grids that increase cyberphysical risks because of the nature of wind and solar generation.

State policies requiring green mandates have resulted in wind and solar constituting about 75 percent of all *new* electricity capacity added to U.S. grids in the past decade (**Figure 13**). This trend creates new pressures on utilities to integrate the vagaries of wind and solar power into their grids, which require power to be available on demand.

FIGURE 13.

New U.S. Generating Capacity



Source: Eaton Blackout Tracker

Yet integrating episodic renewable energy with the continuous need for power—especially with today's surging peak needs—requires an entirely new level of control, integration, and networking. Adding that kind of real-time control with the Internet of Things dramatically increases the opportunities available for cyberattacks—i.e., it greatly expands the "attack surface."

The core issue is the requirement for high-availability energy sources to operate a reliable grid. Today, about 90 percent of America's power comes from readily available sources: 33 percent each from coal and natural gas, 20 percent from nuclear, and 5 percent from hydro dams.[70] Meanwhile, wind and solar power have low average availability. Worse, wind and solar have *zero* availability for many hours each day. Neither wind nor solar output can increase to accommodate surges in peak demand, either.

Solar and wind power can operate successfully thus far *because* of America's surplus of other, high-availability sources. Texas and Iowa, the largest and second-largest wind-generating states, get 70 percent of their electricity from natural gas, coal, and uranium.[71]

Proposals to incorporate vastly more wind and solar on U.S. grids offer essentially two technology solutions to deal with the availability problem: a more networked grid and a grid with far more storage. The former would represent a radical acceleration of the Internet of Things; the latter requires the pursuit of new, radically better, classes of physical chemistry.

Storing large quantities of electricity (**Figure 14**) has frustrated engineers since the dawn of the electric age. Bill Gates, now an investor in a number of new battery companies, has summarized the challenge: "[T]he biggest problem for the two lead candidates [wind and solar] is that storage looks to be so difficult.... We're more than a factor of 10 away from the economics to get [grid-scale storage]."[72]

Figure 14. Battery-Storage Realities

The sheer scale of batteries needed for grid-scale storage (ignoring costs) makes clear the engineering challenge to create U.S. utility systems dominated by episodic power. The total amount of electricity stored at any given moment in all the batteries in America for all purposes—laptops, cars, phones, flashlights, etc.—is countable in just *minutes*' worth of daily U.S. electrical demand.[73]

The enormous $5 billion Tesla battery "gigafactory" under construction in Nevada will produce a quantity of batteries each year that can store 30 billion watt-hours of electricity.[74] Yet that huge quantity of battery supply is a drop in the bucket compared with America's daily consumption of 10,000 billion watt-hours. It would take 100 years for the Tesla factory to manufacture a quantity of batteries capable of storing a half-day's worth of U.S. electric demand.

Utility-scale battery storage has grown nearly 20-fold in only a few years. But that storage still constitutes less than 0.01 percent of overall U.S. grid supply.[75] Even if California, which has America's most aggressive storage mandate, achieved its storage goal by 2020, the storage would provide barely 2 percent of California's peak-power needs.[76]

Regardless of the hopes for breakthrough discoveries in battery technology, there is no realistic prospect for storing electricity as a viable solution to the episodic supply of wind and solar energy.[77] For this reason, green-power advocates view the use of networks (wires) and (smart) network controls as the means to align episodic supply across geographic regions with market demand—combined, as a last resort, with greatly expanded backup from natural-gas generation. But all these solutions greatly increase cyberphysical- and physical-attack surfaces.

More transmission lines (long-haul and local) increase exposures to conventional causes of outages. Increasing the share of U.S. electricity supply coming from natural gas means that it is now important to consider the physical and cyber vulnerability of the gas infrastructure as an additional vector for electric outages. As noted, far greater use of IoT-type network controls also creates a "magnet" for hackers. Finally, it's not just smart meters and other grid IoT devices that are vulnerable. Cyber backdoor exposure is inherent in the control systems embedded in many solar panels and wind turbines themselves.[78]

VII. The State of U.S. Grid Cybersecurity

The prospect of a hacker turning off all of America's lights in a single attack is wildly implausible: to simultaneously bring down all of the country's distributed patchwork of grids (see Figure 4) would be borderline impossible and would, in any case, require nation-state-class capabilities. Even the major 2015 cyberattack on Ukraine's grid affected only about 250,000 residents.[79]

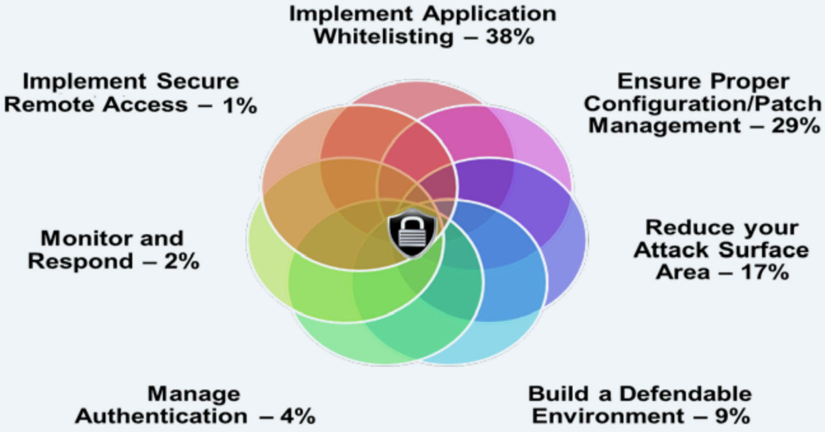
After the Ukraine attack, Gerry Cauley, CEO of the North American Electric Reliability Corporation, testified before Congress,[80] noting, correctly, that U.S. long-haul grids have important technical and operational advantages[81] over Ukraine's (far smaller) grid and that Ukraine was brought back online in only several hours. Though NERC requirements for long-haul grid cybersecurity will escalate in July 2016 with expanded requirements for critical infrastructure protection (CIP) standards,[82] Cauley nonetheless cautioned that U.S. utilities "will need unprecedented levels of financial resources in order to restore their facilities and eventually resume normal operations" after a successful cyberattack.[83]

It is on local U.S. distribution grids—which will not be covered by NERC CIP standards—where the rush is greatest to add Internet-connected devices and green-energy sources. Ironically, while concern over cybersecurity is slowing the adoption of the Internet of Things in many industries, this is not the case for U.S. utilities, which are particularly susceptible to political pressure.[84]

State and federal policies continue to promote or require far greater use of both green energy and Internet-connected smart-grid features. Even though the Energy Policy Modernization Act,[85] passed by the Senate in April 2016 with a bipartisan majority, includes an amendment to the Federal Power Act to authorize the U.S. secretary of energy to "take such actions as the secretary determines will best avert or mitigate [cyber threats],"[86] the bill has several alarming features. It expands and concentrates U.S. cybersecurity authority at the federal level, a development unlikely to boost the speed or flexibility needed to counter such threats. The bill does not cover local U.S. distribution grids, which are far more cyber-vulnerable than long-haul grids. And it expands America's cyberphysical attack surface by promoting the smart- and green-grid transformation already under way.

FIGURE 15.

Seven Strategies to Defend Industrial Control Systems


Implement Application Whitelisting – 38%
Implement Secure Remote Access – 1%
Ensure Proper Configuration/Patch Management – 29%
Monitor and Respond – 2%
Reduce your Attack Surface Area – 17%
Manage Authentication – 4%
Build a Defendable Environment – 9%

Source: U.S. Department of Homeland Security[89]

Consider another example of muddled federal priorities. In December 2015, the Department of Homeland Security issued cybersecurity guidelines[87] (**Figure 15**) for industrial control systems (**Figure 16**). According to the DHS, following the guidelines would have "prevented 98% of the [cyber] incidents reported in FY2015."[88] Among others, the DHS guidelines recommend reducing industrial control systems' attack surface as well as allowing "real-time external connectivity only when absolutely necessary"—a policy at odds with the federal push for smart-greening America's grid.

Figure 16. Industrial Control Systems and the Internet of Things

The digital age of Industrial Control Systems (ICSs) began in 1968 with the invention of the programmable logic controller (PLC). (The Stuxnet virus attack in 2010, against Iran's uranium centrifuges, targeted PLCs, one of the few documented examples of a digital weapon destroying a physical asset.)[90] In 1986, the first PLCs were tied to personal computers; in 1992, PLCs were linked to a local Ethernet using Internet-communications protocols, and in 2003, the first PLCs were embedded in Web servers.[91]

PLCs, sensors, relays, meters, and the like are all connected, monitored, and operated by a supervisory control and data acquisition (SCADA) system, a kind of "industrial Internet" used across industries, especially in the electric sector. While SCADA dates back over a half-century—largely because of the need to operate electrical systems over broad geographic areas—integration with the Internet (whether in factories or on utility grids) is the newest phenomenon in the progression of ICSs.

Today, millions of utility remote terminal units, sensors, meters, actuators, controls, and SCADA systems exist across America's hundreds of local and connected grids, as well as across its long-haul grids. Millions more exist in factories and office buildings—and soon, in homes. And, until recently, ICSs largely existed in operational silos that were far less vulnerable to cyberattack.[92]

U.S. policy schizophrenia on security and green goals is persistent and pervasive. A 2013 White House report[93] that urged greater grid reliability (albeit with a focus on "weather-related outages") also promoted the very technologies that will undermine reliability by expanding grids' cyberattack surface.[94] State policies are no more coherent. New York governor Andrew Cuomo's new "Reforming the Energy Vision"[95] initiative pays lip service to grid security—"[The] availability of reliable, resilient, and affordable electric service is critical to the welfare of citizenry and is essential to New York's economy"—while promoting grid programs that make cyberphysical attacks easier to carry out.

The U.S. Government Accountability Office is not impressed with the state of cybersecurity of America's utility infrastructure, either. In a 2015 report, the GAO warned that:

1. FERC has not taken steps to monitor [the electricity industry's] compliance with voluntary [cybersecurity] standards.
2. Entities in the electricity industry (e.g., utilities) often focused on complying with regulations rather than taking a holistic and effective approach to cybersecurity.
3. Smart grid devices (e.g., meters) did not always have key security features such as the ability to record activity on systems or networks, which is important for detecting and analyzing attacks.
4. The electricity industry lacked sufficient metrics for determining the extent to which investments in cybersecurity improved the security of smart grid systems.[96]

When combined with the rising tech-savviness of groups hostile to America, as well as rising urbanization, federal and state policymakers' prioritization of environmental goals over grid security is making America more exposed to cyberattacks.[97]

VIII. Conclusion

Hackers typically fall into two groups: private individuals or organizations with varying skill levels who hack for financial, nuisance, or harassment motives; and nation-state or nation-sponsored entities with high skill levels that hack for geopolitical motives.

According to CrowdStrike, a cybersecurity consultancy, geopolitical developments have become the "most important drivers for cyberattacks," with the latter now firmly part of the "global threat landscape."[98] Adds Kevin Mandia, CEO of FireEye, another cybersecurity firm: "It does not seem reasonable to expect the majority of the private sector to defend itself from military cyber attacks. We do not expect a homeowner to prevent a military unit from breaking into their bedrooms, so why should we expect companies to prevent or detect similar attacks in cyberspace?"[99]

Dealing with this reality has implications for how federal agencies should work with the private sector and for the appropriate allocation of public resources. The potential for nation-state attacks also has implications for liability protection for utilities in the event of a cyberattack; for sharing classified information with utilities; and for interindustry and interagency coordination. As the GAO reported, the Department of Defense's own infrastructure is vulnerable to cyberphysical attack.[100] Rather than focus on "Climate Change Adaptation Road Maps,"[101] the Pentagon should prioritize helping the private sector secure and defend America's critical electric infrastructure. The Defense Advanced Research Projects Agency announced plans in January 2016 for a $77 million, four-year program to help utilities detect cyberattacks; but given the scale and complexity of the challenges, it is only a small step.[102]

Tech titans, including Facebook, Google, Apple, and Microsoft, have pledged to help advance the deployment of "green" and smart grids.[103] They should also acknowledge, and help resolve, the cybersecurity challenges associated with such initiatives. The foundational responsibility for solutions originates with the technologies' providers, not the users in the industrial and utility sectors. Similarly, investors and policymakers should explore ways to encourage greater focus on innovative venture capital in cyberphysical security—which accounts for less than 1 percent of total venture-capital investment.[104]

As this report argues, if U.S. state and federal cyberphysical security policies are to become coherent and effective, they must be anchored in acknowledging three realities: (1) the rush to make U.S. grids greener and smarter also increases their cyberphysical attack surface; (2) there are two radically different classes of cyber threat: private hackers and nation-state (or nation-sponsored) hackers; and (3) evolving cyberphysical threats are unlike other physical-security issues that utilities have heretofore faced.

Sound grid-cybersecurity policy would therefore:

- Avoid top-down, one-size-fits-all legislation.
- Slow—and, in some cases, halt—smart- and green-grid transformation that increases the attack surface until adequate cybersecurity features are available and incorporated.
- Reallocate grid budgets to increase funding for security, resilience, and reliability, and require cybersecurity metrics as part of pre-deployment requirements for green and efficiency programs.
- Boost utility-sector collaborative engagement with federal cybersecurity programs, especially those of the U.S. Department of Defense.
- Encourage private-sector-led cybersecurity technology research, development, and deployment, so that companies on the front line can move at the speed of innovators, not bureaucrats.
- Ensure that policies, mandates, and regulations in cybersecurity are based on overall objectives—rather than being prescriptive and subject to becoming rapidly obsolete.

Endnotes

[1] 1,000 GW (gigawatts) of installed capacity @ avg. $2,000/kW replacement value = $2 trillion, plus equal value in transmission ($2 trillion) and distribution ($2 trillion). See also http://www.rmi.org/RFGraph-present_value_cost_US_electricity.

[2] See http://www.eia.gov/totalenergy/data/annual.

[3] EIA Annual Energy Outlook 2016, https://www.eia.gov/forecasts/aeo/data/browser/#/?id=47-AEO2016&cases=ref2016~ref_no_cpp&sourcekey=0.

[4] J. R. Minkel, “The 2003 Northeast Blackout—Five Years Later Tougher Regulatory Measures Are in Place, but We’re Still a Long Way from a ‘Smart’ Power Grid,” *Scientific American* (Aug. 13, 2008), http://www.scientificamerican.com/article/2003-blackout-five-years-later.

[5] See https://www.oe.netl.doe.gov/docs/katrina/katrina_083005_1600.pdf.

[6] Mary Williams Walsh and Nelson D. Schwartz, “Estimate of Economic Losses Now Up to $50 Billion,” *New York Times* (Nov. 1, 2012), http://www.nytimes.com/2012/11/02/business/estimate-of-economic-losses-now-up-to-50-billion.html?_r=0.

[7] Billy Ball, “Rebuilding Electrical Infrastructure along the Gulf Coast: A Case Study,” National Academy of Engineering (spring 2006), https://www.nae.edu/Publications/Bridge/TheAftermathofKatrina/RebuildingElectricalInfrastructurealongtheGulfCoastACaseStudy.aspx.

[8] Cited in Minkel, “The 2003 Northeast Blackout.”

[9] Eaton Blackout Tracker Annual Report, Mar. 10, 2016, https://powerquality.eaton.com/About-Us/News-Events/2016/PR100316.asp?id=&key=&Quest_user_id=&leadg_Q_QRequired=&site=&menu=&cx=3&x=12&y=11.

[10] Andy Greenberg, “Hackers Remotely Kill a Jeep on the Highway—with Me in It,” *Wired* (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

[11] Lucas Mearian, “Chrysler Recalls 1.4M Vehicles After Jeep Hack,” *Computerworld* (July 24, 2015), http://www.computerworld.com/article/2952186/mobile-security/chrysler-recalls-14m-vehicles-after-jeep-hack.html.

[12] David Schneider, “Jeep Hacking 101,” *IEEE Spectrum* (Aug. 6, 2015), http://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101.

[13] Teodor Sommestad et al., “SCADA System Cyber Security—a Comparison of Standards,” Royal Institute of Technology (Sweden), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5590215&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5590215.

[14] Devin Coldewey, “Obama Appoints Tech Veterans from Microsoft and Uber to Cybersecurity Commission,” TechCrunch (Apr. 13, 2016), http://techcrunch.com/2016/04/13/obama-appoints-tech-veterans-from-microsoft-and-uber-to-cybersecurity-commission.

[15] Christopher M. Matthews, “Google Search Technique Aided N.Y. Dam Hacker in Iran,” *Wall Street Journal* (Mar. 27, 2016), http://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543.

[16] Steven Cherry, “Stuxnet: Leaks or Lies?,” IEEE Spectrum (Sept. 4, 2012), http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies/?utm_source=techalert&utm_medium=email&utm_campaign=090612.

[17] Lloyd’s Emerging Risk Report, 2015. See https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[18] Sam Shead, “Apple’s Data Centre in Ireland Could Increase the Country’s Electricity Consumption by 8.2%,” *Business Insider* (Apr. 18, 2016), http://www.businessinsider.com/author/sam-shead.

[19] See http://www.tech-pundit.com/wp-content/uploads/2013/07/Cloud_Begins_With_Coal.pdf?c761ac&2b8101.

[20] ~100 billion kWh U.S. data center use per Natural Resources Defense Council, “America’s Data Centers Consuming and Wasting Growing Amounts of Energy,” https://www.nrdc.org/resources/americas-data-centers-consuming-and-wasting-growing-amounts-energy. Re: steel industry ~60 billion kWh, https://www.eia.gov/consumption/manufacturing/briefs/steel.

[21] See http://www.bea.gov/industry.

[22] Ibid.

[23] See http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html?referring_site=RE&pos=2&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[24] Ibid.

[25] Rich Miller, “Internet of Things May Create a New Breed of Data Centers,” Data Center Frontier (May 2, 2016), http://datacenterfrontier.com/internet-things-may-create-new-breed-data-centers.

[26] Peter Judge, “The Truth Is: Data Center Power Is Out of Control,” Datacenterdynamics (Jan. 12, 2016), http://www.datacenterdynamics.com/design-strategy/the-truth-is-data-center-power-is-out-of-control/95425.article.

[27] EIA Annual Energy Outlook 2016, https://www.eia.gov/forecasts/aeo/data/browser/#/?id=47-AEO2016&cases=ref2016~ref_no_cpp&sourcekey=0.

[28] See https://mitei.mit.edu/system/files/Electric_Grid_Full_Report.pdf.

[29] Mary Meeker, Internet Trends 2016, June 1, 2016, KPCB, kpcb.com/InternetTrends.

[30] See http://www.eia.gov/beta/aeo/#/?id=8-AEO2015.

[31] RTOs; otherwise known as Independent System Operators, or ISOs.

[32] See http://about.bnef.com/press-releases/china-out-spends-the-us-for-first-time-in-15bn-smart-grid-market.

[33] See http://create.usc.edu/research/50772.pdf.

[34] Jordan Wirfs-Brock, "Power Outages on the Rise Across the U.S.," IE Inside Energy (Aug. 18, 2014), http://insideenergy.org/2014/08/18/power-outages-on-the-rise-across-the-u-s.

[35] Liz Ronk, "Lights Out New York: The 1959 Blackout," *Time* (Nov. 3, 2012), http://time.com/3874803/new-york-city-blackout-photos-from-the-summer-of-1959.

[36] See http://blog.ucsusa.org/mike-jacobs/2003-northeast-blackout-and-13-of-the-largest-power-outages-in-history-199.

[37] Jennifer Latson, "Why the 1977 Blackout Was One of New York's Darkest Hours," *Time* (July 13, 2015), http://time.com/3949986/1977-blackout-new-york-history.

[38] Sewell Chan, "Remembering the '77 Blackout," *New York Times* blog, http://cityroom.blogs.nytimes.com/2007/07/09/remembering-the-77-blackout/?_r=0.

[39] "The Blackout: Night of Terror," *Time* (July 25, 1977), http://content.time.com/time/subscriber/article/0,33009,919089,00.html.

[40] See http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002006692&Mode=download.

[41] See http://www.eia.gov/todayinenergy/detail.cfm?id=15051#tabs_SpotPriceSlider-8.

[42] "Peak Demand in New York City: What's the Problem?, Feb. 27, 2015, http://www.peakpowerllc.com/notes/2015/2/17/whats-the-problem-with-peak-demand.

[43] See https://www.caiso.com/Documents/FlexibleResourcesHelpRenewables_FastFacts.pdf.

[44] See http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html?referring_site=RE&pos=3&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html, fig. 24.

[45] See http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html?referring_site=RE&pos=3&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

[46] See http://dupress.com/articles/internet-of-things-iot-in-electric-power-industry.

[47] See https://www.navigantresearch.com/research/market-data-iot-for-residential-energy-customers.

[48] Al Sacco, "Cybersecurity Expert and CIO: Internet of Things Is 'Scary as Hell,' " NetworkWorld (Mar. 25, 2014), http://www.networkworld.com/article/2175533/lan-wan/cybersecurity-expert-and-cio--internet-of-things-is---39-scary-as-hell--39-.html?page=1.

[49] Jonathan Camhi, "The New Front in Cybersecurity: How to Prevent Hackers from Taking Down Critical Infrastructure," Business Insider (May 2, 2016), http://www.businessinsider.com/the-new-front-in-cybersecurity-how-to-prevent-hackers-from-taking-down-critical-infrastructure-2016-4.

[50] See http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

[51] See http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf.

[52] Kathy Pretz, "Protecting Critical Infrastructures from Cyberattacks," *The Institute* (Mar. 26, 2015), http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/protecting-critical-infrastructures-from-cyberattacks.

[53] Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired* (Jan. 8, 2015), http://www.wired.com/2015/01/german-steel-mill-hack-destruction.

[54] Fahmida Y. Rashid, "Code Red: Health IT Must Fix Its Security Crisis," InfoWorld (June 2, 2016), http://www.infoworld.com/article/3068179/security/code-red-health-it-must-fix-its-security-crisis.html?token=%23tk.IFWNLE_nlt_infoworld_daily_2016-06-02&idg_eid=df1fe91f6f0013f6b6ae7043a82f47ab&utm_source=Sailthru&utm_medium=email&utm_campaign=InfoWorld%20Daily:%20Morning%20Edition%202016-06-02&utm_term=infoworld_daily#tk.IFW_nlt_infoworld_daily_2016-06-02.

[55] Fred Donovan, "Attackers Targeting Energy, Utilities Sectors to Disrupt U.S. Economy," FierceITSecurity (Dec. 22, 2015), http://www.fierceitsecurity.com/story/infographic-attackers-targeting-energy-utilities-sectors-disrupt-us-economy/2015-12-22?utm_medium=nl&utm_source=internal&mkt_tok=3RkMMJWWfF9wsRoku6zIc%252B%252FhmjTEU5z17OkoXqK1lMI%252F0ER3fOvrPUfGjI4CS8VqMa%252BTFAwTG5toziV8R7LMKM1ty9MQWxTk.

[56] See http://www.tripwire.com/company/research/tripwire-2016-energy-survey-attacks-on-the-rise.

[57] Thomas W. Overton, "Beyond the Firewall: Best Practices for Cybersecurity Risk Management," *Power* (Mar. 1, 2016), http://www.powermag.com/beyond-firewall-best-practices-cybersecurity-risk-management/?hq_e=el&hq_m=3224696&hq_l=22&hq_v=025bb2fcfb.

[58] See https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf. America's utility sector, like its banking sector, must report cyberattacks. Fear of bad publicity may cause other industries to underreport cyberattacks.

[59] NCCIC/ICS-CERT Year in Review, Homeland Security, FY 2015, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

[60] See https://forms.greentechmedia.com/Extranet/95679/forms.aspx?msgid=fdc8fda2-03c4-44cf-9c07-5e3cb4e3b4e1&LinkID=CH00095679eR00000430AD&Source=website.

[61] See http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf.

[62] See http://www.homelandsecuritynewswire.com/dr20160408-the-next-cold-war-has-already-begun-in-cyberspace.

[63] See http://www.prnewswire.com/news-releases/the-state-of-security-in-control-systems-today-a-sans-survey-300102024.html.

[64] See http://www.tripwire.com/company/research/tripwire-2016-energy-survey-attacks-on-the-rise.

[65] AT&T Cybersecurity Insights Report, http://about.att.com/story/cybersecurity_insights_report.html.

[66] See http://ppec.asme.org/wp-content/uploads/2015/11/CleanerCheaperStronger_FINAL_Web.pdf.

[67] See http://www.prnewswire.com/news-releases/the-state-of-security-in-control-systems-today-a-sans-survey-300102024.html.

[68] See https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/reports/50980-EnergySupport_OneCol.pdf.

[69] See http://energy.gov/oe/articles/oe-announces-funding-improve-cybersecurity-nation-s-power-grid State spending: http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf.

[70] See http://www.eia.gov/tools/faqs/faq.cfm?id=427&t=3.

[71] See, for Iowa, http://www.eia.gov/state/?sid=IA#tabs-4; and for Texas, http://www.eia.gov/state/?sid=TX#tabs-4.

[72] James Bennet, "We Need an Energy Miracle," *The Atlantic* (Nov. 2015), http://www.theatlantic.com/magazine/archive/2015/11/we-need-an-energy-miracle/407881.

[73] 260 billion Wh in all batteries (250 billion in car batteries, 9 billion in laptops, 1 billion in smartphones) v. ~400 billion per hour U.S. demand; thus ~30 minutes.

[74] See "Gigafactory Will Cost Tesla $5 Billion but Offers Significant Cost Reductions," *Forbes* blog (Mar. 11, 2016), http://www.forbes.com/sites/greatspeculations/2014/03/11/gigafactory-will-cost-tesla-5-billion-but-offers-significant-cost-reductions; and http://www.teslamotors.com/gigafactory.

[75] Peter Maloney, "Utility-Scale, Long-Duration Markets Take the Lead," Utility Dive (Dec. 22, 2015), http://www.utilitydive.com/news/storage-in-2016-utility-scale-long-duration-markets-take-the-lead/411232/?_hsenc=p2ANqtz--2pAH7DdwbEaxyE5L0TSRSu3J0o2lfS8CR1-QAg75PpnZITraJ3HxfwHME0EYKDN5wukazVSn_fJNjwiOd-jCbXinEX-YUTEyzx2dFbGSeZ9q57XA&_hsmi=24836527.

[76] See http://www.pv-magazine.com/news/details/beitrag/solar-plus-storage-to-become-8bn-market-by-2026--says-lux-research_100022986/#ixzz49Wi2m13c.

[77] Mark P. Mills, "The Tesla and Solar City Merger Is Rooted in Battery Derangement Syndrome," *Forbes.com* (June 25, 2016).

[78] See Peter Fairley, "How Rooftop Solar Can Stabilize the Grid," IEEE Spectrum (Jan. 2015), http://spectrum.ieee.org/green-tech/solar/how-rooftop-solar-can-stabilize-the-grid; and Thomas Fox-Brewster, "Hundreds of Wind Turbines and Solar Systems Wide Open to Easy Exploits," Forbes blog (June 12, 2015), http://www.forbes.com/sites/thomasbrewster/2015/06/12/hacking-wind-solar-systems-is-easy/#2fe3df8427a6; http://www.fas.org/sgp/crs/misc/R43989.pdf; and http://thehackernews.com/2014/10/hacking-smart-electricity-meters-to-cut.html.

[79] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[80] See http://www.nerc.com/news/testimony/Testimony%20and%20Speeches/Gerry%20Cauley%20Testimony%20-%20April%2014%20House%20Transportation%20subcommittee%20hearing.pdf.

[81] See http://www.remotemagazine.com/main/articles/going-beyond-compliance-using-nerc-cip-v5-as-a-catalyst-for-a-greater-security-strategy.

[82] Ibid.

[83] Ibid.

[84] See ibid. and https://www.hubs.biz/power/explore/2015/12/hackers-at-the-gate-part-ii-cybersecurity-experts-say-utilities-must-be-ready-now.

[85] See http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=eb454e3b-7f32-479e-b1a6-e84f9019941d.

[86] See http://www.jdsupra.com/legalnews/passing-of-senate-s-energy-bill-signals-47390.

[87] See https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems.

[88] See http://www.eetimes.com/author.asp?section_id=36&doc_id=1328762&_mc=NL_EET_EDT_EET_industrialcontroldesignline_20160128&cid=NL_EET_EDT_EET_industrialcontroldesignline_20160128&elq=30026fd620c644b6a1599d4c664ec807&elqCampaignId=26709&elqaid=30551&elqat=1&elqTrackId=9b0895ac06b84b5c82bd0920563329ef.

[89] Seven Strategies to Defend ICSs, U.S. Dept. of Homeland Security, https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf.

[90] Kim Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *Wired* (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.

[91] See https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

[92] See https://media.blackhat.com/bh-us-10/whitepapers/Pollet_Cummins/BlackHat-USA-2010-Pollet-Cummings-RTS-Electricity-for-Free-wp.pdf.

[93] See http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[94] See http://breakingenergy.com/2013/08/16/white-house-report-calls-for-increased-electric-grid-resilience/?utm_source=Breaking+Energy&utm_campaign=49e5e09cfa-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_f852427a4b-49e5e09cfa-407307749.

[95] See http://www3.dps.ny.gov/W/PSCWeb.nsf/All/CC4F2EFA3A23551585257DEA007DCFE2?OpenDocument.

[96] See http://www.gao.gov/products/GAO-16-174T.

[97] See, e.g., Katie Bo Williams and Cory Bennett, "Why a Power Grid Attack Is a Nightmare Scenario," The Hill (May 30, 2016), http://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario.

[98] See http://finance.yahoo.com/news/crowdstrike-global-threat-report-analyses-130000072.html.

[99] See https://www.fireeye.com/blog/executive-perspective/2015/12/looking_forward_the.html.

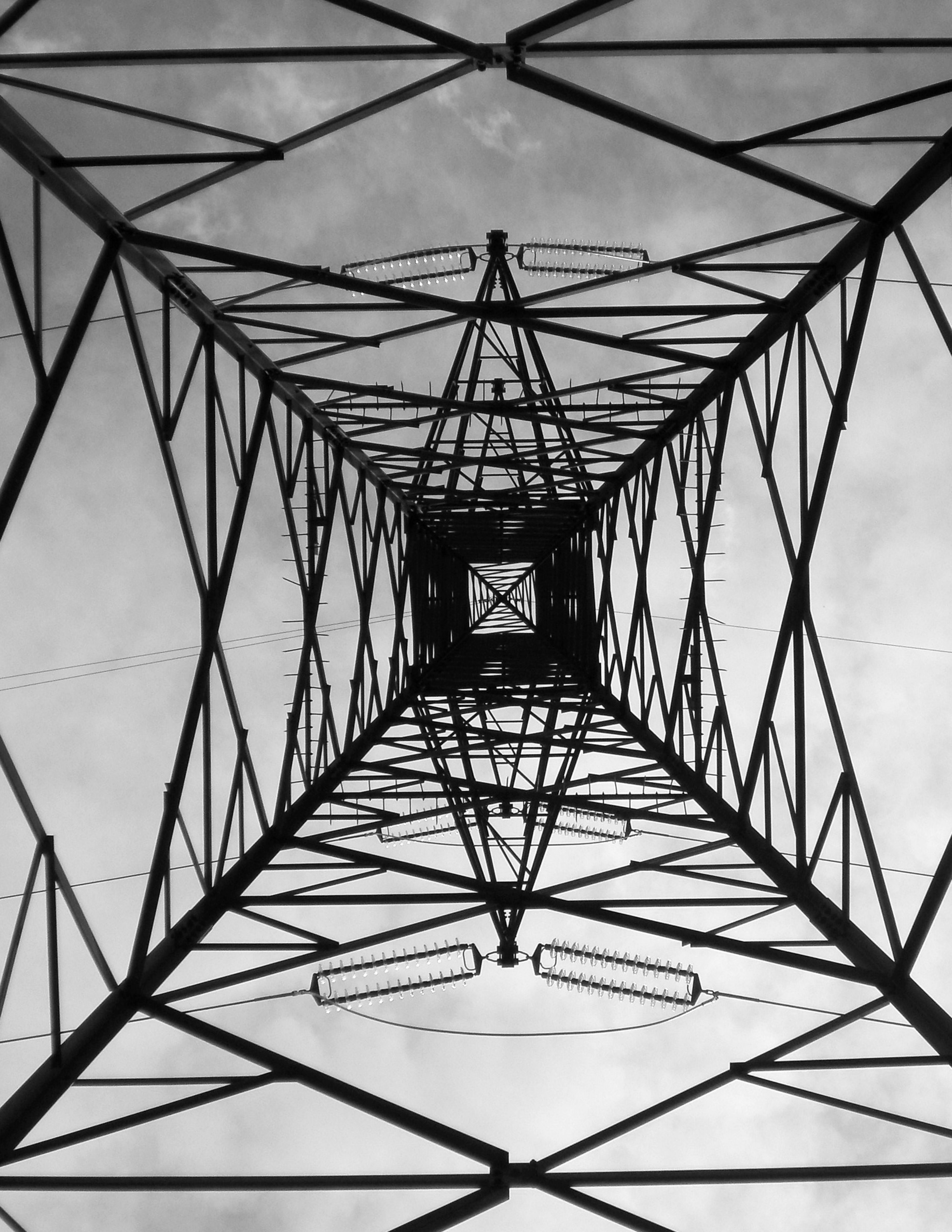
[100] See http://www.gao.gov/products/GAO-15-749.

[101] See, e.g., http://ppec.asme.org/wp-content/uploads/2014/10/CCARprint.pdf.

[102] Christina Maza, "The Pentagon's Plan to Defend the Power Grid Against Hackers," *Christian Science Monitor* (Jan. 25, 2016), http://m.csmonitor.com/World/Passcode/2016/0125/The-Pentagon-s-plan-to-defend-the-power-grid-against-hackers?utm_source=hs_email&utm_medium=email&utm_content=25599773&_hsenc=p2ANqtz-9AhAZmMMUzUk3skD4Jh0eiEYKXixmI9muXyqgeBrfXQLfk8PeQA-Mtp3Iw3EYlv9Cjn6OK0NawMnIjMWngT7I-IK2hrlUauaCzz--D5vZ_QNBBb_M&_hsmi=25599773.

[103] See http://www.smartgridnews.com/story/facebook-work-utilities-develop-green-tariffs-and-more-google-apple-microso/2016-06-06?utm_medium=nl&utm_source=internal.

[104] See http://www.luxresearchinc.com/news-and-events/press-releases/read/venture-funding-cybersecurity-rise-400-million-threats-iot-grow#sthash.GOZ93um6.dpuf.



June 2016

REPORT 16

Abstract

Electric grids have always been vulnerable to natural hazards and malicious physical attacks. Now the U.S. faces a new risk—cyberattacks—that could threaten public safety and greatly disrupt daily life.

Key Findings

1. America's push for "greener," "smarter" grids will involve a vast expansion of the Internet of Things that greatly increases the cyberattack surface available to malicious hackers and hostile nation-state entities.
2. Cyberattacks overall have been rising 60 percent annually for the past half-dozen years, and utilities are increasingly targeted.
3. Federal and state governments genuflect to the goal of reliable, resilient, and affordable electric service; yet comparatively trivial sums are directed at ensuring that grids are more secure, compared with the vast funding to promote, subsidize, and deploy green energy on grids.

MANHATTAN
INSTITUTE