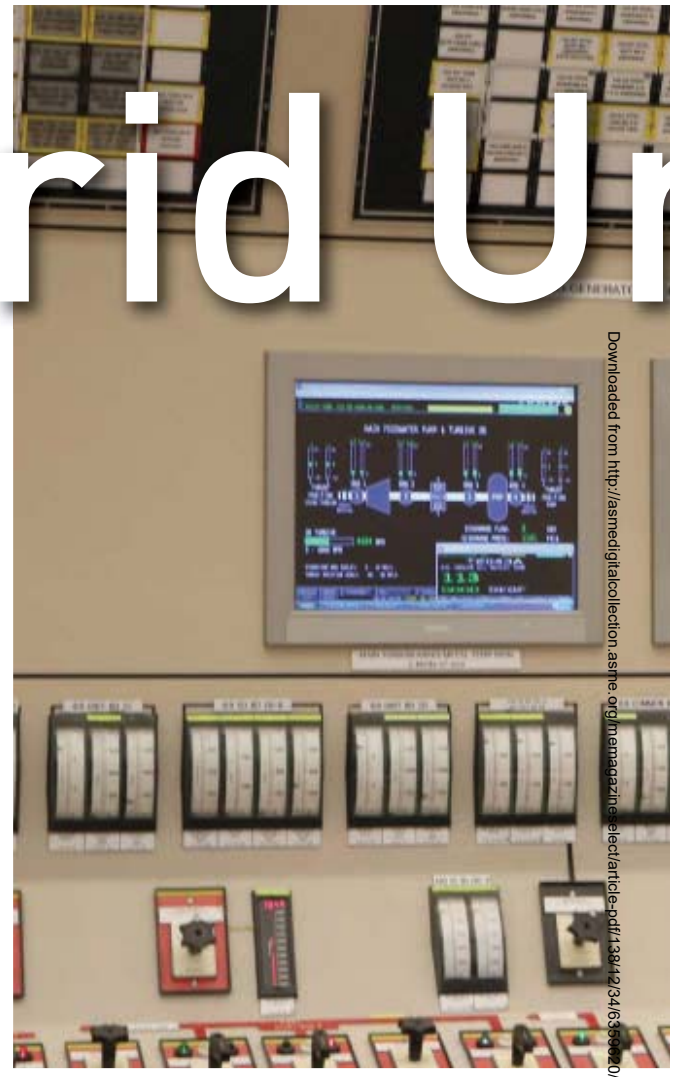
The Grid U



By S. Massoud Amin

On an ordinary afternoon last December, with Christmas just a couple of days away, workers in the Ukraine wrapped up their duties, and families across the nation prepared for the holiday. Then, at 3:30 p.m., as the sun began heading toward the Western horizon, the lights went out.

They went out in a region in the western Ukraine served by a utility called Prykarpattya Oblenergo. A minute later, a second western Ukraine utility lost its power. Then a third. Suddenly, 225,000 people were without electricity.

Before the day was out, Prykarpattya Oblenergo said the blackout was due to outside interference in their system. Soon Ukraine's state security service blamed Russia.

Employees at the three utilities had watched helplessly that day as their operations were hijacked, and in time detective work proved what the utility and the security service had suspected: Malware had homed in on critical equipment and destroyed it, and stealthy human intruders had shut down substations.

In fact, the world had just witnessed the first well-publicized cyberattack that successfully took out a portion of the power grid.

Many people think the electric grid must be securely protected from disabling cyberattack. But while the sky is not falling, many vulnerabilities persist. And now, as the Ukrainian attack made clear, the electric grid has entered a new era of heightened vulnerability.

Our electric power infrastructure supports almost all of our economic and social foundations, including fuel-supply, telecommunications, transportation, and financial networks.

It's also under a lot of stress. Power outages in the United States have increased in size and frequency over the last two decades. Outages and power quality disturbances now cost the economy more than $80 billion annually on average, and sometimes as much as $188 billion in a single year. The grid's ability to safely support anticipated demand has been in question for over a decade.

Meanwhile, the grid is growing more susceptible to cyberattack. Much of the U.S. grid was built out from the 1950s to the 1970s, before modern computer and communication networks, let alone modern security measures. But the grid now relies on computers, many of which were added without considering how they would affect grid operations, and often without adequate cybersecurity.

And as more people generate their own electricity from rooftop solar and other distributed generation technologies, it creates more interconnected nodes on the grid, each with digital sensors, processors, and automated and manual controls. And when the software and hardware at these nodes are not properly configured, hackers can spoof, jam, or hijack them.

Despite the risks, policymakers nationwide are pushing for clean , reliable electricity, and we depend on power and electric grids to grow our

nderFire

Photo: Tennessee Valley Authority

economy, protect public safety, and sustain our daily lives. Therefore, despite these hurdles—or because of them—we must update the nation's end-to-end electric power grid to provide secure, resilient, and reliable electricity for the future.

WEAK LINKS

When investigators conducted their autopsy on the Ukrainian power hack, they uncovered an extremely sophisticated attack—one that showcased several of the more potent weapons utility cybersecurity personnel must contend with.

In the months leading up to the outages, the hackers sent so-called spear-phishing emails to utility workers. The emails appeared to be from friendly sources known to the victims, and asked them to click "enable content" to read an attached document. Some did, and it activated BlackEnergy attack software—a Trojan horse virus that, like the giant wooden horse of Greek legend, appeared innocuous but carried a nasty surprise.

Once activated, BlackEnergy invaded the utilities' office computers, allowing the hackers to root around. They figured out how to access the systems remotely, probably via virtual private network (VPN) connections. And they discovered high-level passwords to computers and industrial control systems that directed utility operations.

When the time was right, the hackers struck. Grid operators watched helplessly as cursors moved around screens, passwords changed, and high-voltage circuit breakers opened at doz-

The grid relies on computers, often without adequate security precautions.

The Ukrainian attack demonstrated the sophistication of today's hackers and the malware they now wield.

ens of substations, causing a blackout.

Nor were the hackers done. They used a program called KillDisk to erase selected files and corrupt firmware to disable entire utility computer systems. They sabotaged restoration efforts by remotely disabling computers needed to repair damaged grid equipment. They even flooded utilities' customer service phone lines with automated calls to prevent customers from reporting the outages.

More than any other publicized attack, the Ukrainian attack demonstrated the sophistication of today's hackers and the malware they now wield. And that malware is being put to use. Today the organizations that manage regional grid operations in North America report 100,000 malicious attempts a day.

To battle crafty hackers and advanced malware, we need advanced cyberdefenses. At the University of Minnesota, we have developed a multilayered set of defenses. Our system spots potential viruses, worms, and other malware and quarantines them into what we call a sandbox that's a virtual replica of the system being invaded.

The hackers think they've invaded our system, but in fact we're safe. And using machine-learning algorithms, we can quietly watch their every move, as if they were lab rats, and learn from their behavior how to fend them off. We also

Cleaning Up

How can a utility make more money by selling less electricity? How can a third-party vendor capitalize on reduced electricity demand? Two innovative companies have created business models to profit on the clean, integrated grid of tomorrow.

Save Now, Charge Later

As electric vehicles become more popular, utilities worry that charging them all at once could overtax the grid. But in San Francisco, EVs actually help the grid on hot days when residents turn on the AC full blast.

That's because automaker BMW helps the local utility, PG&E, meet that electricity demand by delaying at-home charging by 100 owners of BMW's i3 electric vehicles for up to an hour.

"We are working to create an ecosystem for electric cars," said Cliff Fietzek, manager for connected eMobility for BMW of North America. "This is the next step for us to integrate electric cars into the power grid without straining the grid."

Delayed charging was designed to shave 100 kW off peak demand when PG&E experienced a run on electricity. Just in case, a battery at BMW's nearby plant in Mountain View made up the difference in electricity when not enough cars could defer charging.

BMW benefited from the program by burnishing the image of EVs and giving buyers an incentive to drive them. i3 owners got paid up to $1,540.

PG&E benefits as well from this delayed charging program, called iChargeForward, because they don't have to buy or generate power at times of peak demand, when it's most

expensive. At such times many utilities turn to simple-cycle natural-gas peaker plants for a stretch, but these plants are less efficient and emit more polluting carbon dioxide and nitrous oxide than combined-cycle natural-gas power plants, which are utility mainstays.

The response from i3 owners was positive.

learn within seconds how to prevent future attacks—far faster than the weeks or months it now takes to develop and install computer security patches.

Cyberattacks, of course, are not the only security threats that utilities and electric system operators face. Truck bombs or small airplanes can take out substations or even utility operations centers. High-powered rifles can pick off and disable transformers at substations, as happened to a major Silicon Valley substation in 2013.

To protect the electrical system from both cyber and physical attacks, each of its components could in theory be replaced or retrofitted. But the North American grid has 15,000 generators in 10,000 power plants; more than 450,000 miles of high-voltage transmission lines that carry 100 kV or higher and hundreds of thousands more miles of lower voltage lines in the system, so this would be logistically and financially impossible.

Back in the 1990s, however, I realized that there were better ways to protect the grid.

GRID, HEAL THYSELF

Between 1998 and 2002, my team at Electric Power Research Institute and I created and led a large joint research program with the U.S. Department of Defense to make the electric grid smarter and more resilient. The Complex Interactive Networks/System Initiative (CIN/SI) included teams from more than 28 universities, 52 utilities and independent system operators, and the DoD.

We recognized that all of our critical infrastructures–electric, fuel-supply, water, telecommunications, and financial networks–were inter-

More than 500 owners applied for the 100 spots in the 18-month pilot program, and 92 have stuck with it, Fietzek said. It helped that any owner who needed to drive his or her car immediately could opt out of delayed charging, he added.

Even before the program finished, BMW had learned important lessons. From July 2015 to June 2016, PG&E had 134 demand requests. BMW met 94 percent of those requests but needed to call on its Mountain View battery every time, Fietzek said.

iChargeForward ends this month, but BMW is exploring the feasibility of moving from a pilot program to something on a larger scale, Fietzek said. "But to provide 100 kW or more, we're going to need more vehicles," he said.

When the i3 batteries are past warranty and no longer working well enough to effectively charge a car, they can still provide residential charging and storage, and BMW is developing a Second Life Battery program to do exactly that. "Instead of recycling the batteries, it makes much more sense to reuse them," Fietzek said. **ME**

Virtual Power to the People

When a large cloud passes over a solar farm, the electricity supply to the area plummets. Grid managers must act to balance electricity supply and demand, and they must do it fast.

Enbala Power Networks of North Vancouver, B.C., makes software that can generate 20 MW of power within four seconds by simply reaching into the buildings of large commercial and industrial (C&I) users and switching off power-hungry equipment for short periods of time.

Everybody wins. Large C&I users enjoy lower energy bills, courtesy of utility incentives, and usually notice no loss of power. The local utility can quickly respond to changes in demand. Grid operators get the power they needs to meet demand quickly—without the power losses that inevitably occur when drawing from power plants or battery banks.

Enbala profits, too. C&I customers may pay them directly for the service, which is known as a virtual power plant, then manage their own load. Enbala also can bid its virtual power into a lucrative spot market run by the regional energy system operator—then, because of the market's rules, get paid more than they bid.

In effect, Enbala's business model turns the power system upside down, said Enbala founder and CTO, Malcolm Metcalfe. "In the past, generators have always been used to follow the load," Metcalfe explained. "Lots of people turn on lights, and generation ramps up." But Enbala instead adjusts load to match generation.

Let's say a cloud passes over a large array of solar panels, causing a brief loss of 100 MW to the grid. Multiple power providers—a hydro plant, or a coal or gas-fired plant, typically—then bid into the frequency regulation market, which maintains a continuous balance between supply and demand.

Enbala can meet the system's need by immediately reducing power to its customers' air conditioning or refrigerators—far faster than the half hour it can take to ramp up other forms of generation. The system operator pays more to generators that perform faster and better. "We get picked every time," Metcalfe said. **ME**

KAREN QUEEN is a Virginia-based writer.

Our goal was to build a safe, secure, resilient eletrical system that can heal itself when disrupted.

dependent and dynamically coupled. We aimed to judiciously retrofit these infrastructures to make them secure and robust. Because all other infrastructures rely on our power and energy networks, modernizing the electrical grid was central to our efforts.

Our goal—and my goal ever since—was to build a safe, secure, resilient electrical system that can heal itself rapidly when disrupted.

Our strategy for building such a grid emerged from an understanding of how large, complex networks fail. First, a threat or material failure perturbs the network but does not yet pose an emergency. It does, however, force the network into an alert state. The system, which was in a stable equilibrium, begins to lose its balance.

At that point, a well-functioning system will rapidly sense this disturbance and act to regain balance and normal function. But if it can't detect the disturbance in time, or if it can't compensate, the system will enter an emergency state and lose its balance. Part or all of it will then fail.

A self-healing smart grid needs to be supported by secure sensing and communication networks, it needs built-in computational technologies, and it has to be controllable in real time. Ideally, sensors and processors would be built into every working part—every switch, every circuit breaker, every transformer, every busbar. These devices would also need built-in communications technologies to speak with each other and with grid command centers, and they'd need built-in physical and cyber security defenses.

Such a system would also need centralized intelligence. For example, an intelligent and secure layer of devices would monitor the health of a substation's equipment and automatically report electrical problems or disruptive cyberattacks to a local control center on a college campus or in an industrial park. Alternatively, if a cyberattack disabled equipment on a substation in a microgrid—a local, mostly self-sufficient power system connected to the larger grid—the microgrid would automatically disconnect from the grid to localize the problem and fix it before reconnecting.

The sensing and communication technology on far-flung grid elements would give command-and-control centers better situational awareness. They could use this to plan for future conditions.

A grid that was truly smart, secure and self-healing, would make for fewer and shorter power outages. It would detect abnormal signals that indicate equipment failure or a brewing thunderstorm, and they would reconfigure the system to isolate disturbances or at least minimize their impact. It would detect and override human errors that can cause power outages.

To remake today's electrical system, we'll need more technology development. At the University of Minnesota, for example, we are designing, modeling, and assessing control architectures that enable the power grid to respond quickly to natural disasters, equipment failures, physical attacks, and cyberattacks. We're also testing them on an experimental microgrid and conducting cost-benefit analysis of options, designs, and policies.

And the existing grid will have to be retrofit. This would be expensive, but its benefits would far outweigh its costs. By investing about $20 billion a year for 20 years, smartening the grid would, by conservative estimates, generate $2.80 to $6 to the economy for every dollar invested.

Such a grid would prevent damage to all the other infrastructures that depend on a working electrical grid. It would allow the electrical system to safely integrate more renewable power from rooftop solar panels, small-scale wind, and other clean technologies. It would create jobs, foster a globally competitive workforce, and enable a 21st century infrastructure that supports a digital society with increased power demands. In fact, it's a must for the United States to remain an economic power.

And the next time bad actors conspire on a grid-disrupting cyberattack, the new grid might just make for a more peaceful holiday. ME

S. MASSOUD AMIN, an ASME fellow, directs the Technological Leadership Institute at the University of Minnesota and is regarded as "the father of the smart grid."