THE AMERICAN PROSPECT IDEAS, POLITICS & POWER

MONEY, POLITICS AND POWER CORONAVIRUS CIVIL RIGHTS IN AMERICA FAMILY CARE LAW AND JUSTICE DAY ONE AGENDA
HEALTH AND SOCIAL POLICY ENERGY AND THE ENVIRONMENT + HOUSING AND TRANSPORTATION + WORKING IN AMERICA +
AMERICA AND THE WORLD ECONOMIC POLICY THE PROSPECT ARCHIVE + POLITICS GREEN NEW DEAL CABINET WATCH
FIRST 100

The Power's On, for Now

Modernizing the electric grid delivers efficiencies but opens up security challenges.

BY GABRIELLE GURLEY JUNE 14, 2021

KARL-JOSEF HILDENBRAND/PICTURE-ALLIANCE/DPA/AP IMAGES

The COVID-19 crisis cratered the American economy in a few months, but a coordinated assault on the electric grid could do great damage in a week or less.

If people with bad intentions crossed the Mexican and Canadian borders to raid American towns, or landed unseen on coastal beaches to launch guerrilla attacks, the country would mobilize to get on a war footing in no time. But Energy Secretary Jennifer Granholm admitted earlier this week that those actors are already among us, just not in physical form. We saw a hint of the chaos they can wreak when Colonial Pipeline shut down in a ransomware attack; electric grids are also vulnerable. “We’ve got to up our game,” Granholm said.

The COVID-19 crisis cratered the American economy in a few months, but a coordinated assault on the electric grid could do great damage in a week or less. But pandemic-weary Americans aren’t interested in electric grid vulnerabilities. Neither are members of Congress. President Biden proposed $100 billion in electric transmission system upgrades, but in the first round of negotiations, Republicans showed up with zero dollars for the grid. Those negotiations later fell apart. A new “gang” of five Democratic and five Republican senators has reportedly reached agreement on a mildly bigger “hard” infrastructure package, but there are no details on what it will cover, and no guarantee grid upgrades will be included.

More from Gabrielle Gurley

As electric utility companies step back from fossil fuels and incorporate more wind and solar resources into electric power generation, the push to modernize the electric grid could plug some of these vulnerabilities, even as it creates others for black-hat hackers to exploit. But even if cybersecurity weren’t an issue, grid upgrades would be desperately needed for our climate and economic future.

Three major grids deliver electricity to the lower 48 states; two of them are known as “interconnections.” The Eastern Interconnection delivers power to the Eastern states south to Florida, a section of northern Texas, and west all the way to the Rocky Mountains. (It also serves the eastern and central Canadian provinces, excluding Quebec, which has its own grid.) The Western grid serves the states on the other side of the Rockies (and British Columbia and Alberta). Texas has ERCOT, a self-contained grid for most of the state. Texas officials segregated the system from the other two to avoid federal regulation, a decision that prevented Texas from securing additional power during the February deep freeze that paralyzed most of the state.

> “
> The Colonial Pipeline attack is the up-our-game moment.

Within the major grids are independent system operators and regional transmission organizations that manage electricity markets and coordinate power supplies. Public and private electric utilities and rural electric cooperatives run the distribution networks that furnish electricity to home and business consumers. Overall, “the grid” balances supply challenges to periods of peak demand and severe weather events, from heat waves to cold snaps.

Most Americans get power from a small number of investor-owned utility companies. These companies have stepped up generation, transmission, and distribution investments, but not enough to meet the roughly $200 billion needed to keep up with technology and ongoing maintenance demands. The average age of power transformers is 25 years; for transmission lines, it's over 30. The Los Angeles Department of Water and Power's (LADWP) Power Plant One, a hydroelectric facility, is more than a century old.

Electric generation modernization programs demand major adaptations, such as new transmission pathways to accommodate renewable generation. Permitting these lines can take two to three years and get undone by community objections and other obstacles. But they are essential to getting renewable-energy plants online.

Another focus of modernization is storage for intermittent sun and wind energy; to keep power flowing throughout the day regardless of the weather, it's critical to be able to maintain reserves when it's cloudy, dark, or still. California is the national leader in solar generation and energy storage solutions. More than a decade ago, state lawmakers and energy officials kicked off an ambitious program for microgrids, storage, and smart-grid improvements.

At the consumer level, California ratepayers can get incentives to use batteries to store excess energy generated by rooftop solar systems for use in the evenings. San Diego, the primary center for utility-grade storage solutions, saw the deployment of infrastructure developer LS Power's Gateway Energy Storage project, the country's largest battery storage system, in early June.

Smart-grid technologies help operators manage the additional energy demands of consumer-generated power that is sold back to the grid. They also alert consumers and operators to potential trouble spots in the networks, and facilitate recovery from weather-related emergencies. This brings us back to cyber threats. Both the smart grid and the "internet of things" (which includes smart appliances, thermostats, and other devices in the home) introduce state-of-the-art but hackable systems all along the electricity generation/transmission/distribution networks.

> “Even if cybersecurity weren't an issue, grid upgrades would be desperately needed for our climate and economic future.

There are two simultaneous trends at work in grid modernization, says Stuart Madnick, an information technologies professor and director of cybersecurity at the MIT Sloan School of Management. "You have an irreversible trend to connecting more things to the internet, then you have people recommending that the energy systems be disconnected from the internet," he says. Even "air gaps"—disconnecting systems from the internet—do not offer complete security. Madnick notes that computers hit by the 2010 Stuxnet malware attack on Iran's nuclear program were not connected to the internet.

"Occasionally, you'll talk to executives in companies, particularly energy-type companies, and they'll say, 'We feel very secure because we are air-gapped,'" Madnick adds, "as if they think that makes them invulnerable."

The Colonial Pipeline attack is the up-our-game moment. Unlike investor-owned electric utilities, which must share information about attacks, oil and gas companies were not subject to federal sharing protocols that cover cyber intrusions. "Sharing promotes readiness," says Tracey Woods, vice president for operations with the American Association of Blacks in Energy. "Black hats are going through their checklists and collecting ransom from companies with the same profile."

In response to the Colonial case, the Transportation Security Administration (TSA), which oversees pipelines, has directed pipeline operators to notify the agency of "malicious software and unauthorized access to [information technology/operational technology] systems and physical attacks on the network structure." Companies that aren't household names think that hackers only go after big targets. "[Colonial] thought they were out of sight, out of mind," Woods says.

In April, Senate Energy and Natural Resources Committee chair Joe Manchin (D-WV) and Sen. Lisa Murkowski (R-AK) introduced a bill that would direct the Federal Energy Regulatory Commission to incentivize utilities to invest in new cybersecurity technologies, and create a grant and technical assistance program for rural cooperatives, municipal utilities, and small investor-owned firms.

The modernization push combined with the Colonial Pipeline episode should lead electric utilities to assess their vulnerabilities. They won't do it without prodding though. As Woods says, "If the regulators do not prioritize and [insist] that cybersecurity is beneficial to customers, who should then pay for the upgrades, investor-operator utilities will not do these improvements on their own." That's where federal funding can come in as a carrot for upgrades. But so far, the money's been left on the table.

GABRIELLE GURLEY

Gabrielle Gurley is The American Prospect's deputy editor.