Free markets. Real solutions.

R STREET SHORTS NO. 36
September 2016

HOW MICROGRIDS COULD HELP PROTECT TEXAS

Josiah Neeley

INTRODUCTION

Reliable electricity is vital to civilization. By harnessing the power of electricity, countries like the United States have achieved historically unprecedented levels of prosperity and human advancement. Growth in electricity consumption and economic growth traditionally have gone hand in hand. While increased energy efficiency has blunted that relationship somewhat in recent years, there's no question that ready access to electricity is a foundation for modern society.

But the electrical grid's critical role in the economy also serves as a source of vulnerability. Should the grid fail – whether due to deliberate attack, an accident or a natural event – the results could be catastrophic. Without electricity, simple everyday tasks such as pumping gas, withdrawing money from a bank account or talking with a loved one in another state would become difficult, if not practically impossible.

Even isolated and temporary loss of electricity can be economically damaging and life-threatening. These dangers rise exponentially as the duration and geographic range of the power loss expands.

Virtually every sector of the U.S. economy relies on electricity. As the U.S. EMP Commission noted in 2004:

> All of the critical functions of US society and related infrastructures—electric power, telecommunications, energy, financial, transportation, emergency services, water, food, etc.—have electronic devices embedded in most aspects of their systems, often providing critical controls.[1]

Each of these sectors relies not only on electricity, but on each other. For example, a functioning food supply depends on functioning transportation; both, in turn, depend in the long term on a functioning financial system, which relies on functioning telecommunications, and so forth. Failures in any one sector are likely to compound failures in the others, which in turn become vastly more destructive the longer electricity remains inaccessible.

The current grid also relies heavily on key pieces of infrastructure that are difficult to repair or replace. For example, bulk transmission of electricity relies on large power transformers, which weigh between 200,000 and 800,000 pounds and must be custom-designed and built.[2] Replacing a large power transformer is a daunting task during ordinary times, and could prove all-but-impossible if other systems were likewise impaired.

The consequences of an extended disruption of the electrical grid are almost too frightening to contemplate. Even relatively minor disruptions could have serious economic and security consequences. Given the stakes, it's imperative the State of Texas take reasonable measures to increase the resilience of its electrical grid. Even low-probability scenarios – some of which might seem far-fetched at first glance – must be taken seriously and guarded against to the extent practicable.

This paper reviews a number of emerging threats to a functioning electrical grid. It also highlights one way to protect against these threats: increased use of distributed generation. A decentralized grid offers protection by reducing the likelihood that failure of any particular central point or installation would bring down the entire system.

EMP WEAPONS

An electromagnetic pulse (EMP) is a short intense burst of electromagnetic energy. Such bursts can disrupt the functioning of electronic devices, causing voltage surges that

temporarily short-circuit electrical equipment. The extent and range of interference depends on the level of the EMP. At a sufficiently high enough, an EMP can permanently damage or destroy key electrical components.

EMPs' threat to the electrical grid is twofold. First, an EMP could damage grid equipment. Second, given the integrated nature of the grid, the sudden loss of this equipment could result in a cascade of failures, in turn leading to widespread power loss.

An EMP can be generated by several types of natural or man-made phenomena. However, when it comes to concerns about the electrical grid, the most commonly envisioned scenario involves an EMP generated by a high-altitude nuclear explosion. Because of the extreme intensity of such an explosion, a single high altitude nuclear EMP could disrupt electric functionality throughout much of the continental United States.

The extent of damage from a high-altitude EMP was accidentally demonstrated during the nuclear tests of the 1950s and 1960s. In 1962, a nuclear test at an altitude of approximately 400 kilometers over the Pacific Ocean caused electrical disruption 1,400 kilometers away in Hawaii. The EMP generated by the explosion resulted in "the failure of streetlighting systems, tripping of circuit breakers, triggering of burglar alarms, and damage to a telecommunications relay facility."[3] Similar testing by the Soviet Union was found to have damaged underground cables as far as 600 kilometers from the blast location.

Smaller EMPs also can be produced by non-nuclear explosives. While the range and intensity of these EMPs would be far smaller than with a nuclear-produced EMP, such weapons still could impair electrical systems and could be an attractive option for terrorist organizations.

SOLAR EMPS

In addition to the risk from EMPs used as weapons by hostile actors, similarly disruptive phenomena sometimes occur naturally. A coronal mass ejection – sometimes called a "solar EMP" – is a large ejection of plasma and magnetic field from the sun. These ejections can then be carried into space on "solar winds," the continuous flow of charged particles from the sun. CMEs are a daily occurrence and, in most cases, have no effect on the Earth. But if a sufficiently large CME hit the Earth's magnetosphere, it could cause the same disruptions to electricity as a weaponized EMP.

In 1859, the planet was hit by a large solar storm known as the Carrington Event. At the time electricity was not widely in use. Nevertheless, the storm caused widespread failures in telegraph systems throughout Europe and North America.[4]

In 2012, a similarly sized CME barely missed hitting Earth. Had this solar storm hit the planet's magnetosphere, insurance underwriters have estimated it would have caused between $600 billion and $2.6 trillion in damage.[5] A subsequent analysis found there is a 12 percent chance of a Carrington-sized solar storm hitting the Earth at some point between 2014 and 2024.[6]

Smaller CMEs have hit Earth, causing disruptions to the electrical grid, albeit on a smaller scale. In 1989, a solar storm knocked out power to parts of Quebec. While areas like Texas that are farther from the poles are less at risk from a CME, the prospect of an event remains a real concern.

CYBERHACKING AND CONVENTIONAL ATTACKS

The electrical grid could also be brought down by more targeted attacks on infrastructure used to manage and maintain grid stability. As a study by the National Research Council has noted:

> Modern power systems rely heavily on automation, centralized control of equipment, and high-speed communications. The most critical systems are the supervisory control and data acquisition (SCADA) systems that gather real-time measurements from substations and send out control signals to equipment, such as circuit breakers.[7]

This makes the grid vulnerable to a variety of cyberattacks, as coordinated cyberattacks on the grid "could entail costs of hundreds of billions of dollars." As the study further noted:

> If they could gain access, hackers could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems. ... [A] cascading outage would be aggravated if operators did not get the information to learn that it had started, or if protective devices were disabled.[8]

Low-tech attacks also are possible. On April 16, 2013, unidentified assailants attacked the Metcalf Transmission Substation outside San Jose, California. Using AK-47 assault rifles, the attackers managed to disable 17 large power transformers before escaping. While the attack failed to produce blackouts, it showed signs of professionalism and planning.[9] Some, including former Federal Energy Regulatory Commission Chairman Jon Wellinghoff, have suggested the attack could have been a dry run for potentially larger operations.[10]

ACCIDENTS AND STORM DAMAGE

On Aug. 13, 2003, power went out throughout much of the Northeast United States and parts of Canada. The blackout

was the result of a software glitch that failed to alert operators about the need to redistribute power due to downed powerlines. While most power was restored within two days, even this temporary shutdown caused ripple effects throughout the economy. Offline refineries caused an estimated 10 cents a gallon rise in the price of gasoline. Overall, the blackout may have cost as much as $10 billion in damage and lost economic activity.[11]

The 2003 blackout shows that not all threats to the grid involve terrorism or intentional sabotage. Accidents, carelessness and even natural disasters like hurricanes can render large areas without power. Earlier this summer, the governor of Louisiana had to be evacuated from the governor's mansion after flooding had cut electric power to the residence.

PROTECTING THE GRID

There is no single strategy that will protect the grid against all potential threats. Preventing terrorist attacks on critical infrastructure like electricity is, of course, the responsibility of law enforcement, as well as the nation's intelligence community. States should nonetheless take reasonable precautions to increase the resilience of the grid in case of attack. Precautions must also be taken against natural threats, whether in the form of CMEs or destructive storms.

Grid infrastructure can be modified to protect it from EMPs and CMEs. This hardening process is moderately expensive, but not prohibitively so. But even an EMP-hardened grid would still be vulnerable to cyberattacks and other forms of sabotage.

An alternative way to protect the grid is to make it less centralized. In 2012, for example, U.S. Rep. Roscoe Bartlett, R-Md., introduced a resolution that, among other things, asked that "every community and institution begin to reestablish its ability to generate at least 20 percent of its own power for its critical infrastructure and services in order to provide its citizens with food and water."[12]

Others have promoted similar ideas. Ex-FERC Commissioner Jon Wellinghoff has discussed the advantage of distributed generation to promote grid resilience by making it more difficult to bring down the whole grid through attacks on centralized nodes:

> If everyone had solar panels on their respective roofs then we could adequately disperse power generation in such a way that it makes nodes practically irrelevant. It is easy to hack into a node and cause it to malfunction but it is basically impossible to hack 10 million solar power systems.[13]

Distributed generation has been growing rapidly in Texas due to falling costs and technological improvements. However, certain regulatory barriers remain to further growth.[14] Given the potential increased resilience to grid attacks that distributed generation could provide, the Legislature and regulators should be careful not to impose burdens that hamper the continued growth of this sector.

CONCLUSION

There is no such thing as absolute safety. Society will always face new threats, and the fact that a grid failure would be so devastating is, in a way, a testament to the huge benefits the modern electrical grid provides. Nevertheless, where steps can be taken to minimize risk at reasonable cost, it would be reckless not to do so. Texas should take reasonable precautions to harden the risk against attack and should allow the grid to evolve in the direction of greater decentralization.

ABOUT THE AUTHOR

Josiah Neeley is senior fellow and Southwest region director for the R Street Institute. He has worked extensively on energy and environmental issues, including federal air quality regulation, climate change, water markets, oil and gas production, renewable energy and electricity.

Josiah was previously a policy analyst for the Center for Tenth Amendment Studies and the Armstrong Center for Energy & the Environment at the Texas Public Policy Foundation.

ENDNOTES

1 John S. Foster Jr., et al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Vol. 1: Executive Report 2004," p. 8, July 22, 2004. http://www.empcommission.org/docs/empc_exec_rpt.pdf

2 Patricia Hoffman and William Bryan, "Large Power Transformers and the U.S. Electric Grid," Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, April 2014. http://energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf

3 EMP Commission 2004, p. 4.

4 Committee on the Societal and Economic Impacts of Severe Space Weather Events, "Severe Space Weather Events – Understanding Societal and Economic Impacts," National Research Council Division on Engineering and Physical Sciences Space Studies Board, 2008. http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf

5 Lloyd's and Atmospheric and Environmental Research Inc., "Solar Storm Risk to the North American Electric Grid," May 2013. https://www.lloyds.com/-/media/lloyds/reports/emerging%20risk%20reports/solar%20storm%20risk%20to%20the%20north%20american%20electric%20grid.pdf

6 Tony Phillips, "Near Miss: The Solar Superstorm of July 2012," Science@NASA Headline News, July 23, 2014. http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/

7 Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack, "Terrorism and the Electric Power Delivery System," National Research Council Division on Engineering and Physical Board on Energy and Environmental Systems, Nov. 25, 2012. https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system

8 Ibid.

9 Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," Wall Street Journal, Feb. 5, 2014. http://www.wsj.com/articles/SB10001424052702304851104579359141941621778

10 Ted Koppel, "Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath," Crown, First Edition, p. 19, Oct. 27, 2015.

11 ICF Consulting, "The Economic Cost of the Blackout: An Issue Paper on the Northeastern Blackout, August 14, 2003," 2004. http://www.solarstorms.org/ICFBlackout2003.pdf

12 H.Res. 762, "Expressing the sense of the House of Representatives regarding community-based civil defense and power generation," 112th Congress, Aug. 2, 2012. https://www.govtrack.us/congress/bills/112/hres762/text

13 Chip Register, "Former FERC Chief Jon Wellinghoff Speaks Out on Grid Security and Distributed Generation," Forbes, Feb. 3, 2015. http://www.forbes.com/sites/chipregister1/2015/02/03/former-ferc-chief-jon-wellinghoff-speaks-out-on-grid-security-and-distributed-generation/5/#5379568a1a97

14 See, e.g., Josiah Neeley "Improving the market for Clean Energy in Texas," R Street Institute, April 2016. http://www.rstreet.org/policy-study/improving-the-market-for-clean-energy-in-texas/