We Are One Terrorist Attack Away from A Major Nationwide Blackout: What Should We Do?

Ephram Glass
Smart Grid Consulting

Victor Glass
Rutgers University

Abstract

Securing critical infrastructure from sophisticated cyber and physical attacks is a top national priority. As recent attacks on the Ukraine electric grid and Metcalf substation have demonstrated, coordinated and sophisticated attacks are a real threat to the nation's electric grid. A well-planned and executed physical attack on critical substations can cause widespread blackouts that would last for months. Blackouts of that length would cripple the U.S. economy. This paper reviews government and industry initiatives to improve grid resiliency and shows that the current strategies are not sufficient to protect the nation's electric grid. The authors propose a plan for reducing the number of critical substations through a combination of government mandates and market incentives to bring power generation closer to customers.

Introduction

One of the top priorities of a society is to protect itself from attack. In 1948, just three years after World War II, Edgar M. Hoover reflected on what locational policies could provide adequate national security against the threats of modern weapons. He wrote that before cannons, towns were perched on rocky hilltops surrounded by high walls.[1] As weapon technology advanced, walls no longer provided adequate protection and by the 1930s, countries started placing their heavy industry far from their borders to protect themselves from a potential attack.[2] However, Hoover pointed out

that modern weapons have now essentially eliminated safe areas and that the only options left were to put critical infrastructure underground or to disperse it.[3]

While the U.S. electrical grid is primarily above ground, it had been fairly dispersed until the past few decades. When the electrical utility industry started to develop in the late nineteenth century, hundreds of small utilities each had their own local generation. Rapid technological change in the early twentieth century rapidly reduced the number of utilities producing a national grid with a handful of grid interconnections and generation plants built far from cities making the U.S. electrical grid vulnerable to failures of key substations.[4]

The potential losses from a physical attack on the nation's grid could stimulate the push towards distributed generation and use of renewable resources to generate power while simultaneously propping up some nuclear and coal generators that are no longer cost-competitive. The threat could serve as an impetus to reform state and federal regulations and initiatives that often conflict with each other.

The threat of low-tech physical attacks on the nation's grid infrastructure gets far less attention than the threat of cyberattacks, which are typically considered the preferred weapon for bringing down the grid.[5] Governments and other politically motivated groups continue to wage cyberwarfare to compromise or cripple critical infrastructure including the electric grid. These threats are credible considering the 2015 cyberattack on Ukraine that led to widespread outages and recent Russian cyberattacks against U.S. infrastructure.[6, 7]

Other threats to the U.S. electric grid are not war-related. The 2003 Northeast blackout and the 2011 Southwest blackout were caused by a combination of weather, poor maintenance, and human error.[8-10] Paradoxically, both the successful cyberattack in Ukraine and the major blackouts in the U.S. have one feature in common: power was restored to most customers within 24 hours.[11-13] As a policy, most utilities return to manual control in the event computer systems are compromised, which is why cyberattacks can only cause somewhat brief blackouts. In contrast, physical attacks to the infrastructure can result in widespread blackouts that last for months.[14] If a well-planned physical attack were successful, it could cripple the U.S. economy.

In the aftermath of the 2013 sniper attack by a team of gunmen on PG&E's Metcalf substation, the U.S. government realized that a physical attack was a credible threat to the electric grid.[15] The Metcalf substation attackers targeted the high-voltage transformers to cripple them beyond repair. The electric grid uses high-voltage transformers to raise voltages for efficient

transportation of electricity. If enough transformers are taken out of service, the remaining transformers would be unable to supply enough power to load centers such as cities, towns, and manufacturers. Luckily, in the case of the Metcalf substation attack, enough nearby generation and power line capacity was available to keep everyone in service while only a few neighborhoods lost power temporarily.[16]

In response to the Metcalf substation attack, the Federal Energy Regulatory Commission (FERC) conducted a study to determine what it would take to cripple the electric grid.[17] They identified thirty critical substations where removal of any nine would cause a collapse of the electric grid. Moreover, if the high-voltage transformers at those critical substations were damaged beyond repair, it could take months to fully repair the system. In response to the study's findings, FERC mandated utilities add significantly more security around and in critical substations.[18] In 2018, Congress reevaluated the security measures being taken by utilities and concluded that the grid is more secure than it was in 2013 but was still vulnerable to a sophisticated physical attack.[19]

This paper will show that some of the base assumptions for securing the grid recommended by FERC are not sufficient to make the grid resilient to physical attack. An alternative, discussed in this paper, is to decentralize generation, thereby lessening the reliance on high-voltage transformers. The remainder of this paper is organized as follows: Section 2 describes why the grid is so vulnerable to physical attack. Section 3 reviews solutions proposed to secure the electric grid. Section 4 explains why current security measures are not adequate. Section 5 reveals how market forces can be used as tool for securing the grid. The last section concludes with the suggestion that a combination of short-term and long-term solutions would provide the best security for the grid while simultaneously appeasing factions that support different portfolios of energy generation.

Why is the electric grid so vulnerable?

Grid vulnerability traces back to basic assumptions about the likelihood of network failure used by utilities and system operators. They are responsible for running and maintaining a resilient electric grid. To do this, they perform load flow and stability studies to ensure that each conductor, transformer, and every other electric device does not exceed its capabilities. These studies are primarily done on expected peak summer load, peak winter load, and light load cases where the generation dispatch is varied.[20, 21] In addition to checking the normal state of the electric grid, these studies also check contingencies where certain pieces of the grid are taken out of service for maintenance, equipment failures, faults, or stuck breakers.[22]

Contingencies that remove one element in the grid are called N-1 contingencies, removal of two are N-2, etc. Removal of two elements in the grid consecutively where the grid is allowed to recover from the first removal is called an N-1-1 contingency. System operators and utilities rarely perform load flow and stability studies beyond N-1-1 because removal of more elements from the grid is considered to be highly improbable.[23] When these improbable events do happen on critical lines, it has a large effect. Both the 2003 Northeast blackout and the 2011 Southwest blackout occurred because of scenarios well beyond N-1-1.[24-26] FERC's own study of resiliency of the electric grid to physical attacks took at least a N-1-1-1-1-1-1-1-1-1 contingency (removal of nine substations) to bring the grid down. Any well-planned attack of the electric grid will be well beyond the N-1-1 contingencies system operators and utilities plan for in their routine studies.

The most expensive and vital equipment holding the electric grid together are in substations. They can house high- voltage transformers (345 kV and up) that are instrumental in transmitting electricity from large generators to large load centers like cities.[27] These transformers are custom built for very specific installations by only a handful of manufacturers, most of whom are overseas.[28] Building and replacing a high-voltage transformer usually takes between 5 and 16 months but sometimes takes much longer. Due to their large size and their custom design for each substation, these high-voltage transformers cannot easily be swapped between substations. Besides the long lead-time for building, transporting, and installing these transformers, they are not built to withstand deliberate attacks.[29]

Over the past century, the electric grid has relied more heavily on higher voltages, and the supporting transformers, to transport power from generators built more frequently far from cities and other residential areas.[30] Lower siting costs and NIMBYs have driven large nuclear, oil, gas, and coal powered generators to remote, rural areas. With today's de-regulated power markets, the costs for transporting electricity are borne by electricity consumers, so the distance to large load centers is not a strong factor in generator placement.[31, 32] Adding to the incentive to build generators in remote areas, transmission companies earn more by building more high-capacity, high-voltage lines to transport distant generation to load centers.[33] Once new transmission lines are built, the incentive to build generation capacity at the ends of the line increases because of the reduced likelihood of generation curtailment caused by transmission line congestion.[34] The main limit on this reinforcing feedback loop for remote power generation is the amount of load growth and the number of generators retiring near load centers. Despite these constraints, as more generation is built far from load centers, more substations become critical to supporting the electric grid.

Unless the incentive to build far from the electric loads is diminished or removed, there will continue to be critical substations (and transformers) that are key to supporting the electric grid.

What solutions have been proposed?

There have been several solutions proposed to protect the critical substations from physical attacks. These solutions address physical access, availability of spare transformers, redundant connections within the grid, increased distributed generation, and information security.

To address physical security of substations, some utilities have installed opaque walls to replace the standard chain-link fences surrounding their critical substations to block line-of-sight into the substations specifically to prevent low-tech sniper attacks.[35] They have also installed FERC mandated security cameras facing outward and inward at critical substations to identify suspicious activity outside a substation and to identify intrusions. Some utilities have begun posting guards 24/7.

Another suggestion for decreasing accessibility to critical substations is by building "bunker substations" that are compact, enclosed and may be placed underground or in camouflaged buildings.[36] However, converting existing substations to a more compact design is tremendously expensive and difficult to execute; therefore utilities have not been seriously considering this option.[37]

Several government and industry initiatives were started to address the vulnerability of high-voltage transformers. The Department of Homeland Security funded a program to develop a recovery transformer that was adaptable to various grid installations.[38] Edison Electric Institute (EEI) instituted a multi-utility spare transformer program that shares spare transformers between utilities.[39] The Department of Energy proposed a Strategic Transformer Reserve to ensure a supply of high-voltage transformers was available in the event of an attack.[40] Manufacturers have also started selling armored transformers that are more resilient against physical attacks.[41] However, to date, the only program that's had moderate significant progress has been the EEI spare sharing program.[42] While the Department of Homeland Security succeeded in building an adaptable transformer design, only the test transformers have been placed in service.

The FERC guidelines for increasing grid resiliency include building additional lines and substations.[43] While several utilities have added this option to their planning criteria, few are seriously considering it.[44] The cost to build additional substations and transmission lines is very high and providing a convincing cost-justification to utility commissions would be difficult.

Increasing distributed generation has been proposed as a means to remove the risk to the electric grid.[45] Adding generation near load centers would remove the need to ship generation long distances, effectively eliminating critical substations. However, this option has not been considered by the U.S. government or the utilities. This may be primarily due to the lack of a viable mechanism to execute this option. It is the responsibility of the utilities and system operators to ensure the electric grid does not collapse, but with increasing deregulation of the power market, they have limited ability to influence the siting of generators.

One of the primary lines of defense the U.S. and utilities are relying upon is keeping the identity of critical substations secret.[46] The people tasked with identifying and reviewing critical substations are subjected to background-checks and load flow data is only available to regional transmission organization (RTO) members. This defense assumes load flow data is highly secure and impervious to cyberattacks.

Why the proposed solutions won't be effective

In response to attacks on substations and FERC mandates, utilities have concentrated on preventing the kind of attack executed at Metcalf substation. The solution, as previously mentioned, includes opaque walls around the critical substations, cameras and proximity alarms, and increased coordination for sharing high-voltage transformer spares.[47] While a Metcalf-type attack has been the most sophisticated attack on the U.S. electric grid to date, it pales in comparison to the sophistication behind the 2015 attack on Ukraine's electric grid.

Although the Ukraine event was caused by a cyberattack rather than a physical attack, it showed a high level of electric grid knowledge and it used low-tech hacks of IT administrators to gain admin privileges to multiple systems.[48] While the Metcalf attackers knew that transformers were vulnerable, they lacked operational knowledge that could have allowed them to execute a more effective, coordinated attack on the grid.

Three elements are needed for a successful physical attack on the grid: a mechanism for the physical attacks, identification of critical substations, and knowledge of the design vulnerabilities of substations. Critical substations are primarily air-insulated. In other words, the conducting elements that connect equipment and lines are open to the air in large substations. While a wall might prevent snipers from shooting through the fence of an air-insulated substation, they cannot prevent remote operated drones with IEDs duct taped to them from zipping over a substation wall and blowing up a transformer. IED enabled drones have been used successfully by ISIS in Iraq and started to be used by Mexican drug cartels and even an assassination

attempt on the president of Venezuela.[49-51] The extra cameras, alarms, and even posted guards would not be able to do much against such an attack.

A successful attack would require knowledge of the critical substations. While the U.S. may be banking on keeping that data a secret, that information is often public or easily obtained. For one, the entire transmission grid with all mapped lines and substations is downloadable and even published by the U.S. government.[52, 53] Air-insulated substations are readily viewed on satellite maps where large transformers can easily be identified. Anyone with enough time can make a rough load flow model of the U.S. electric grid with just that topological data and access to the internet. However, doing that would be unnecessary because RTOs will provide their load flow data freely to its members.[54-57] Due to deregulation of the electricity market, generators and even retail customers need access to load flow data to efficiently participate in the market. Any truly sophisticated attack would include masquerading as a generator or customer to gain access to load flow data.

Given that there is both a viable mechanism for a physical attack and an easy means to obtain the key data to identify critical substations, a sophisticated physical attack on the U.S. electric grid would be relatively simple to execute. Attackers would only need a handful of people with IED-equipped drones and someone capable of performing load flow analysis. The Ukraine cyberattack shows that knowledgeable people can be behind sophisticated attacks on the grid; ISIS shows the viability of IED-equipped drone attacks. It is not hard to imagine an anti-American country or terrorist organization using coordinated drone attacks to cripple the electric grid.

What should be done?

Considering the ease of implementing a successful attack on the electric grid, the current proposed solutions to protect the grid fall very short. Returning to Edgar M. Hoover's example, utilities are walling substations like people did hundreds of years ago. They focus on hardening the target and having reserves nearby to resupply when attacked. Walled cities didn't provide adequate protection when cannons were invented; similarly, walled substations won't work in a world with IED-equipped drones.

In reality, the best way to protect the substations that are critical to supporting the electric grid from physical attacks, or even cyberattacks, is not to have critical substations in the first place. A proposed solution that would effectively declassify substations from the critical list is to increase distributed generation. With generation close to the load, it would be very difficult to cause the cascading outages that cause widespread blackouts.[58]

Generation can get sited near load through three methods: market incentives, mandates, and subsidies.

Economic siting of a new generator balances expected returns against costs that can include construction costs, environmental and archeological surveys, public outreach, real-estate purchases, interconnection fees, and other infrastructure upgrades. In some respects, transmission congestion in today's deregulated markets provides incentives to build generation capacity close to load centers. When dispatching generation, system operators are required to use generators near load centers to avoid overloads on constrained, or congested, lines. This provides profit opportunities to site generators near or in large load centers because they can charge higher prices than would be the case if the system was not congested (Lesieutre & Eto, 2003, p. 6).[59, 60] Deregulated markets use congestion pricing to factor in the need to use higher priced generation in congested zones. These additional congestion costs are then passed on to customers through higher electricity rates. In practice, the incentive to build generation in congested zones is often undercut by transmission line upgrades or new construction built to reduce the congestion causing the higher prices. This significantly increases the risk of building new generation near load centers because added transmission capacity would cut their expected generation revenue. In contrast to deregulated markets, vertically integrated, regulated utilities do not have that type of revenue risk because they have a unified generation and transmission plan. Their generation siting regulations simply stipulate that they build the least-cost option while balancing renewable mandates and public support.[61]

Recent government subsidies have increased installations of wind farms, solar farms, and rooftop solar and have also been proposed to prop up existing coal and nuclear generation that would otherwise be uncompetitive.[62] However, only the latter subsidies have been proposed for the sake of national security. A significant portion of government renewable energy subsidies go to rural wind and solar farms, which continues the trend of siting generation far from load. To achieve more distributed generation, different approaches would be needed for regulated markets and deregulated markets. For vertically integrated utilities in regulated markets, the government can mandate that the utilities place new generation close to load centers with the intent of eliminating critical substations. Since these utilities are regulated and don't have to compete with other generation, integrating a national security factor into their generation siting process would be relatively straightforward.

However, in deregulated markets, mandates don't play a direct role. For instance, RTOs must respond to state renewable mandates, but RTOs cannot

mandate specific amounts of renewable generation; they can only make it easier for renewable generation to participate in the market.[63] In deregulated markets, market clearing prices in combination with market design are the primary drivers for adding new generation and for indicating where siting generation would be most lucrative. For deregulated markets, a more effective solution would be to set market clearing prices based on a generation dispatch that takes transmission capacity limitations into account while also minimizing substation criticality.[64] While today's markets already factor in capacity constraints into congestion pricing, minimizing substation criticality would be a new pricing factor. The market should include signals to raise generation prices in zones where transport of electricity into those zones causes substations to become critical to the stability of the electric grid. The resulting market clearing prices will increase revenues to generators in congested zones while reducing revenues to generators in uncongested zones.[65] Inclusion of this "critical substation" factor in the electricity market would increase profitability of new generation in congested zones while discouraging additional generation outside of congested zones. Over time, as more generation is built closer to the load; no substations will need to be classified as critical to the grid.[66]

As a result of higher market clearing prices where critical substations exist, local coal and nuclear power plants currently struggling in today's market may become cost competitive again. However, while higher prices in congested zones would incentivize significant investment in local generation, there would still be pressure from NIMBYs that would hamper new fossil fuel and nuclear generation from being built. These two factors would likely cause an increase in offshore wind farms and solar installations, particularly rooftop solar. However, while the overall effect of changing the electricity market may increase renewable generation, it may actually halt renewable generation development in some areas. Plains States with renewable mandates may rely on a build-out of wind farms that have high wind generation potential. Changing the electricity market to incentivize local generation would make out-of-state wind farm generation appear more expensive and would likely curtail its development.

The growth in renewable generation is already incentivizing a significant built-out of energy storage, particularly batteries.[67] An additional price boost to eliminate substation criticality should reinforce this trend. Without adequate storage, in congested zones with renewable energy credits like California, market prices swing dramatically between high load periods and light load periods where high amounts of renewable generation can cause negative market clearing prices, yet positive revenue to subsidized generation.[68, 69] The negative prices caused by excessive local generation have

prompted proposals to build additional transmission lines to export the excess electricity to neighboring states.[70] However, adding a "critical substation" factor into the market may negate the benefits of building additional lines to alleviate congestion. A countervailing effect of the large price swings from low or negative prices to high peak prices would make the energy storage market more lucrative.[71] For instance, energy storage providers would get paid to store the excess energy while prices are negative and then get paid again when they sell that stored electricity during peak demand. While large pumped-hydro facilities function as energy storage on the grid today, regulatory reform to enable homeowners to tap into the energy storage market would trigger a significant built-out of in-home batteries which would further disperse energy infrastructure contributing to a more secure grid.

All these indirect effects of adjusting the electricity market to factor in national security would not be a quick fix to the vulnerability of the grid. On average it takes several years for any generator to go from a proposal to actually generating power. In the interim, a combination of the solutions currently being considered needs to be implemented to fill the gap as well as providing subsidies to maintain existing plants in load centers that would otherwise retire and go out of service.

Conclusion

Securing critical infrastructure from sophisticated cyber and physical attacks is a top national priority. As recent attacks on the Ukraine electric grid and Metcalf substation have demonstrated, coordinated and sophisticated attacks are a real threat to the electric grid. FERC's study of critical substations has shown that a well-planned and executed physical attack can cause widespread blackouts that would last for months. Blackouts of that length would cripple the U.S. economy.

To make the grid more resilient against unforeseen attacks, the U.S. needs to increase distributed generation to ensure no substations are critical to the stability of the electric grid. In regulated markets, utilities should be mandated to site new generation to minimize and ultimately eliminate substation criticality. For deregulated markets, electricity markets should include a factor to minimize substation criticality. The resulting increase in market clearing prices will provide direct price signals to increase generation supply that will in turn reduce the number of critical substations. In the interim, the U.S. should continue to pursue a combination of solutions. Grid resiliency can be boosted by providing subsidies to prevent existing plants located in load centers from retiring and by purchasing, stockpiling, and coordinated sharing of critical high-voltage transformers. Adding substation

monitoring and intrusion protection provides additional grid protection. By using both these short-term solutions and the longer-term solution of adding distributed generation, the U.S. can effectively mitigate cyber and physical attacks on the electric grid. As side effects to securing the electric grid, these solutions will support local coal and nuclear generating plants while simultaneously incentivizing a significant increase in renewable energy. These side effects may be enough of an incentive to get enough bipartisan support to make these crucial changes to secure our electric grid.

Authors

Ephram Glass is an independent utility consultant specializing in smart grid services and enterprise asset management. In his thirteen years in the industry, he has worked on load growth planning, renewable energy and demand response regulatory affairs, generator interconnections, compliance, cyber security, transmission and distribution automation, reliability, analytics, asset accounting, resource management, and project management. He earned a Bachelor of Science degree in Electrical Engineering from Princeton University.
email: ephramglass@gmail.com

Victor Glass is Director, CRRI Scholar, and Professor of Professional Practice - Finance and Economics, Rutgers Business School - Newark and New Brunswick, Rutgers University. Prior to joining Rutgers, Dr. Glass was Director of Demand Forecasting and Rate Development at the National Exchange Carrier Association. For almost thirty years, he was responsible for forecasting demand and setting switched and special rates for more than 1100 telephone companies. He was heavily involved in access restructure, universal service reform, and new access services. He is the lead author of many business and academic studies. Dr. Glass earned his MBA in marketing and finance, and Ph.D. in economics from Columbia University.
email: vglass@business.rutgers.edu

Endnotes

1. Hoover, E. M. (1948). *The location of economic activity*. NY: McGraw-Hill.
2. Ibid.
3. Ibid.
4. Pomp, R.D. (2000). A brief history of the electric utility industry. In P. Burling (Ed.), *Impacts of electric utility deregulation on property taxation*. Cambridge, MA: Lincoln Institute of Land Policy.
5. Douris, C. (2018, January 16). As cyber threats to the electric grid rise, utilities and regulators seek solutions. *Forbes*.
6. Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*.
7. Tatum, S. (2018, March 17). U.S. accuses Russia of cyberattacks on power grid. *CNN*.

8. Federal Energy Regulatory Commission, & North American Electric Reliability Corporation (2012). Arizona-Southern California outages on September 8, 2011: Causes and recommendations. Washington, D.C.: Federal Energy Regulatory Commission.
9. Northeast blackout of 2003. (n.d.). *Wikipedia*.
10. 2011 Southwest blackout. (n.d.). *Wikipedia*.
11. Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*.
12. Northeast blackout of 2003. (n.d.). *Wikipedia*.
13. 2011 Southwest blackout. (n.d.). *Wikipedia*.
14. Smith, R. (2014, March 12). U.S. Risks national blackout from small-scale attack. *The Wall Street Journal*.
15. Parfomak, P. W. (2014). Physical security of the U.S. power grid: High-voltage transformer substations (Publication No. R43604). *Congressional Research Service*. Washington, D.C.: Federation of American Scientists.
16. Koerth-Baker, M. (2018, August 13). Hacking the electric grid is damned hard. *FiveThirtyEight*.
17. Smith, R. (2014, March 12). U.S. Risks national blackout from small-scale attack. *The Wall Street Journal*.
18. FERC. (2014). Physical security reliability standard Order No. 802. Washington, D.C.: Federal Energy and Regulatory Commission.
19. Parfomak, P. W. (2018). NERC standards for bulk power physical security: Is the grid more secure? (Publication No. R45135). *Congressional Research Service*. Washington, D.C.: Federation of American Scientists.
20. Baseline reports [Corporate website]. *PJM*.
21. A generation dispatch is a set of generators generating power while others are offline. Only the amount of generation to meet the load requirement is dispatched.
22. A "stuck breaker" condition is one where a breaker fails to trip due to a fault. As a result, the next set of isolating devices must trip to isolate the fault.
23. NERC Reliability Standards. (2015). Transmission system planning performance requirements (Publication No. TPL-001-4). *North American Electric Reliability Corporation*.
24. U.S.-Canada Power Systems Outage Task Force (2004). *Final report on the August 14, 2003 blackout in the United States: Causes and recommendations*. Washington, D.C.: U.S. Department of Energy.
25. Northeast blackout of 2003. (n.d.). *Wikipedia*.
26. 2011 Southwest blackout. (n.d.). *Wikipedia*.
27. Parfomak, P. W. (2014). Physical security of the U.S. power grid: High-voltage transformer substations (Publication No. R43604). *Congressional Research Service*. Washington, D.C.: Federation of American Scientists.
28. Ibid.
29. Ibid.
30. Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in the North American power grid. *The European Physical Journal B*, 46, 101-107.
31. An acronym for "not in my back yard" that's used to characterize people opposed to the siting of something perceived as unpleasant or dangerous in their local area.

32. Lesieutre, B. C., & Eto, J. H. (2003). Electricity transmission congestion costs: A review of recent reports (Publication No. LBNL-54049). Washington, D.C.: U.S. Department of Energy.
33. 2017 Transmission investment [Organization website]. (2017). *Federal Energy and Regulatory Commission.*
34. Farber-DeAnda, M., Bratvold, D., Hennessy, T., Hoffman, D., & Fuller, T. (2007). Overcoming transmission constraints: Energy storage and Wyoming wind power. *U.S. Department of Energy.* Albuquerque, NM: Sandia National Laboratories.
35. Parfomak, P. W. (2014). Physical security of the U.S. power grid: High-voltage transformer substations (Publication No. R43604). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
36. Ervin, P. (2017, October). *Build a small energy bunker not a large fortress.* Proceedings at the NERC E-ISAC Grid Security Conference. St. Paul, Minnesota.
37. Parfomak, P. W. (2018). NERC standards for bulk power physical security: Is the grid more secure? (Publication No. R45135). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
38. Parfomak, P. W. (2014). Physical security of the U.S. power grid: High-voltage transformer substations (Publication No. R43604). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
39. Ibid.
40. U.S. Department of Energy. (2017). Strategic transformer reserve: Report to Congress march 2017. Washington, D.C.: U.S. Department of Energy.
41. Parfomak, P. W. (2018). NERC standards for bulk power physical security: Is the grid more secure? (Publication No. R45135). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
42. Parfomak, P. W. (2014). Physical security of the U.S. power grid: High-voltage transformer substations (Publication No. R43604). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
43. NERC Reliability Standards. (2015). Physical security: Standard development timeline (Publication No. CIP-014-2). *North American Electric Reliability Corporation.*
44. Parfomak, P. W. (2018). NERC standards for bulk power physical security: Is the grid more secure? (Publication No. R45135). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
45. Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in the North American power grid. *The European Physical Journal B,* 46, 101-107.
46. Parfomak, P. W. (2014). Physical security of the U.S. power grid: High-voltage transformer substations (Publication No. R43604). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
47. Parfomak, P. W. (2018). NERC standards for bulk power physical security: Is the grid more secure? (Publication No. R45135). *Congressional Research Service.* Washington, D.C.: Federation of American Scientists.
48. Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired.*
49. Houck, C. (2017, October 26). The Pentagon's IED-hunters have a new target: Drones. *Defense One.*

50. Joyce, K. (2017, October 25). IED attached to drone in Mexico could show evolution of drug cartel tactics. *Fox News*.
51. Venezuela President Maduro survives 'drone assassination attempt'. (2018, August 5). *BBC News*.
52. U.S. state profiles and energy estimates: U.S. energy mapping system [Digital image]. U*.S. Energy Information Administration*.
53. Electric power GIS data [Corporate website]. *MAPSearch*.
54. Membership enrollments [Corporate website]. *PJM*.
55. PJM. (2018). PJM manual 14B: PJM region transmission planning process revision 42. Valley Forge, PA: PJM.
56. Customer registration [Corporate website]. *ISO New England*.
57. ISO New England. (2018). Request data and information [Corporate website]. *ISO New England*.
58. Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in the North American power grid. *The European Physical Journal B*, 46, 101-107.
59. Lesieutre, B. C., & Eto, J. H. (2003). Electricity transmission congestion costs: A review of recent reports (Publication No. LBNL-54049). Washington, D.C.: U.S. Department of Energy.
60. Locational marginal prices (LMP) are typically higher in high load, congested zones and lower in less urbanized, uncongested zones.
61. Lesieutre, B. C., & Eto, J. H. (2003). Electricity transmission congestion costs: A review of recent reports (Publication No. LBNL-54049). Washington, D.C.: U.S. Department of Energy.
62. DiChristopher, T. (2018, June 1). Trump administration moves to keep failing coal and nuclear plants open, citing national security. *CNBC*.
63. Pfeifenberger, J., Chang, J., Aydin, O., & Oates, D. L. (2016). The role of RTO/ISO markets in facilitating renewable generation development. Cambridge, MA: The Brattle Group.
64. This assumes non-uniform market clearing prices. If uniform market clearing prices are used, there's little incentive for generation to be built. Most RTOs no longer use uniform market clearing prices.
65. Demand response located in load centers would also benefit from this change to the market. For the purposes of this paper, demand response is considered to be a generation source.
66. When no substations are considered critical anymore, the market clearing prices will only be affected by transmission capacity constraints.
67. Zhou, Y., Scheller-Wolf, A., & Smith, S. (2016). Electricity trading and negative prices: Storage vs. disposal. *Management Science. 62*(3), 880-898.
68. Ibid.
69. Renewable energy credits are subsidies that are paid per kWh of renewable energy generated. When there is more generation available than load, a renewable generator may bid a negative amount (i.e. pay to produce energy) in order to continue receiving renewable energy credits. They would still receive a positive cash flow since the subsidy would be more than they pay for continuing to produce electricity.
70. Arenchild, M. (2018). *Planning the western grid : Impact of new policies and technology*. Paper presented at 31st Annual Western Conference of the Center for Research in Regulated Industries (pp. 1-32), Newark, NJ.

71. Farber-DeAnda, M., Bratvold, D., Hennessy, T., Hoffman, D., & Fuller, T. (2007). Overcoming transmission constraints: Energy storage and Wyoming wind power. *U.S. Department of Energy*. Albuquerque, NM: Sandia National Laboratories.