SMRs a Promising Solution to Long-Term Blackouts Threatened by Cyber, EMP, and Climate Events

Micala Gillespie

Spring 2019

CAI
CENTER FOR ANTICIPATORY INTELLIGENCE

COLLEGE OF HUMANITIES AND SOCIAL SCIENCES
UtahStateUniversity

SMRs a Promising Solution to Long-Term Blackouts Threatened by Cyber, EMP, and Climate Events

Center for Anticipatory Intelligence
Student Research Reports

Micala Gillespie
April 2019

Executive Summary

The national and economic security of the United States depends on reliable electric grid infrastructure, but despite growing vulnerability to long-term energy blackouts by cyberattack, manmade and natural electromagnetic pulse (EMP), and extreme weather driven by climate change, infrastructure stakeholders lack incentives to coordinate national strategies on key threats and recovery objectives as well as the implementation of protective measures and backup energy sources. As the power grid supports every other sector of society, American security demands **(1)** improved interstate planning to anticipate and navigate the effects of long-term, widespread blackouts, **(2)** incentives for private utility owners and operators to invest in risk mitigation, and **(3)** longer-lasting, more resilient backup energy sources and infrastructure to ensure that critical areas can maintain function even when the larger power grid has failed. Reducing the catastrophic consequences of large-area, long-duration grid failures is a problem of imagination and incentives, but not of economic, political, technical, or social feasibility. As such, this report recommends best practices for strengthening human governance practices as well as the resilience of physical systems, with an emphasis on Small Modular Nuclear Reactors (SMRs) as a viable tool.

This report compiles an open-source analysis of cyber, electromagnetic pulse, and extreme weather threats to the US electrical grid system, followed by available policy avenues to mitigate the consequences of large grid failures. The focus of this analysis is on threats that are likely to result in long-duration, large-region energy loss, defined as those that persist longer than the life of backup energy supplies and cover a region so large that significant outside assistance is impractical.[1] Enhancing electric grid resilience will require **(1)** incentivizing risk mitigation for high-consequence, low-probability events, **(2)** encouraging assessments of interdependent control and communication systems, and **(3)** improving physical system resilience by investing in Small Modular Nuclear Reactors—currently the only source of energy which can offer a safe, carbon-free, reliable, and independent power source able to withstand cyberattack, EMP, and natural disaster. If taken seriously, these measures will significantly advance system resilience, ensuring that the electric grid and the society it powers are able to absorb disruption in a way that minimizes the magnitude of service failure.

Introduction: Electric Grid Vulnerabilities Risk Major-Scale Blackouts

The electrical grid in the United States comprises all electricity generation, transmission, distribution, and control systems, but as infrastructure reaches retirement age and energy demand grows, this grid—which underpins every other sector of American society—is increasingly vulnerable to long-duration, large-region power loss from cyberattack, EMP, and climate change. Increasing the nation's capacity to restore power quickly to military and civilian sectors after malicious or natural disruption will require public-private interstate alignment on key threats and recovery objectives, enhanced incentives to "harden" critical components, and investment in more resilient, diverse redundancy measures including Small Modular Nuclear Reactors (SMRs).

Cyber Threat Exacerbated by Investment in "Smart" Grid Technology

Although the electric grid supports nearly every other critical US infrastructure and the potential of a devastating cyberattack on the US power grid represents a high-likelihood and high-consequence scenario, "smart grid" modernizations hyper-vulnerable to cyberattack continue to receive the bulk of the Department of Energy's (DOE) and industry's attention and investment. Smart grids stabilize the grid by using digital communications technology like smart meters, smart appliances, and energy efficient resources to detect and react to local changes in usage. What was once a three-region grid system serving regional needs with *one-way flows* of electricity from individual power plant to consumer is now becoming an interconnected "smart" system with *two-way flows* enabling **(a)** automatic outage detection and service restoration, **(b)** massive interstate energy transfers, and **(c)** flexible use of small-scale energy generation like solar, wind turbines, biomass generators, and battery storage[2] (all referred to as Distributed Energy Resources or DERs).[3] However, features that make smart grid modernizations attractive, including cloud or ethernet-based services and intelligent electronics,[4] also make them vulnerable by providing more entryways for cyberattack.[5]

Grid modernization vulnerabilities are most commonly posed by supervisory control and data acquisition (SCADA) systems and internet portals, allowing attackers to remotely take control over control centers that ensure reliable service and safety and then feed systems false data to physically damage components. The latter vulnerability was demonstrated by domestic white-hat hackers (people who find cyber vulnerabilities in a system before malicious actors can) having the capacity to destroy full wind farms by directing turbines to spin the wrong direction, reminiscent of the Stuxnet malware attack on SCADA systems within the Iranian nuclear complex at Natanz.[6] Adversaries deploying similar techniques against the US power grid could not only cut off power to American homes and entities but could also alter and steal information, disrupt economic activities, and challenge public perceptions of safety and confidence in government. While no major attacks have yet occurred on the US bulk power system, adversaries continue to lay the groundwork for future exploitation by carrying out detailed reconnaissance and establishing remote access or malware,[7] benefitting from cyber intrusions too small to provoke major US retaliation. The varied intent and degree of intrusion depends on the actor, though Russia, China, Iran, and North Korea present the most likely sources of attack.[8] Terrorists and

non-state actors have been assumed to present a less likely threat in their capacity to carry out high-consequence attacks,[9] but should not be discounted.

Russia has shown itself as more than willing to lay cyberattack foundations years in advance and target the ethernet-based protocols that are now becoming standardized in US smart grid technology.[10] In 2014 the Russian malware "BlackEnergy" was discovered on Ukrainian energy sector networks,[11] and in both December 2015 and December 2016 Russia used this malware to cut off power to hundreds of thousands of Ukrainians in the dead of winter. Russia took control from a remote location, then proceeded to overwrite the substations' internet communication protocols, preventing legitimate operators from regaining control and damaging backup control station batteries.[12] Given that Russia has already probed and inserted malware in the US grid infrastructure as it did in Ukraine,[13] that it was reported in 2018 to have shifted its focus towards demonstrating an ability to disrupt the US electric utility grid instead of midterm elections,[14] and is preparing its own domestic front for the potential of a massive cyberattack,[15] it is likely that Russia might seek to exploit US energy infrastructure vulnerabilities.

China has also used software programs to map the US power grid,[16] and often uses blunt force cyber tools such as network scanners, viruses, and botnets to intrude on US critical infrastructure SCADA control systems.[17] While these intrusions begin with espionage, it is likely China is also developing capabilities to attack the power grid. For example, Chinese military personnel charged in 2014 for stealing US economic secrets were also linked to the hacker pseudonym "UglyGorilla" responsible for cyber intrusions on a northeastern US utility company going back to 2012.[18] Though China has historically not favored direct, first-strike attacks on infrastructure, its cyber sophistication and growing tension with the United States suggest the potential for a limited attack or first-strike attack on the American electric grid should be considered a credible threat by grid infrastructure owners and operators.

Iran may be less sophisticated than the former two states in capability, but may have stronger real intent to attack.[19] In one of the largest state-sponsored hacking campaigns ever prosecuted by the Department of Justice (DOJ), nine Iranian hackers were indicted with hacking into hundreds of US computer systems, including the Federal Energy Regulatory Commission's database and a New York dam.[20] This is especially worrisome in that Iran believes that it has a right to retaliate for what is believed to be a US-conducted Stuxnet attack on the SCADA systems controlling its nuclear infrastructure,[21] as well as for the 2018 US withdrawal from the Joint Comprehensive Plan of Action (JCPOA or Iran nuclear deal). Given Iran's aspirations to develop nuclear infrastructure largely for economic benefits and the centrality of the US grid for economic security, Iran may see attacks on US grid infrastructure as an economic weapon proportional to that of the STUXNET attack and US JCPOA withdrawal. Given that Iran typically responds proportionally in a "tit-for-tat" fashion,[22] evidenced by Iranian cyberattacks on US banks and a New York dam after the discovery of STUXNET,[23] heightened tensions with Iran over economic sanctions and nuclear enrichment would likely leave its leaders feeling justified to retaliate by disrupting US electricity infrastructure. Iran's decision in May 2019 to ease its adherence to the nuclear deal as the US moves B-52 bombers, anti-missile defense, and a Navy strike group into the region[24] suggest that tensions are likely to heighten in the coming months, making the hardening of smart grid modernization components to Iranian cyberattack a high-priority task.

Though smart grid integration with the main grid offers exceptional control, cost-efficiency, and resilience to common disruptions, catastrophe may be enabled or exacerbated if smart grid modernizations continue without a central focus on inherent cybersecurity and a clear picture of the evolving system's weak spots. The Department of Homeland Security (DHS), Department of Energy (DOE), and private electric utility officials would find it in their best interest to ensure grid resiliency with **(1)** private-public alignment on threats and risk-mitigation, **(2)** incentives to design inherently secure smart grid technology, and **(3)** an expansive knowledge of vulnerable components and single point of failure (SPOF) units where one piece's failure can lead to broader system failure. In doing so, American energy infrastructure may be better able to absorb cyberattacks without permanent damage, minimize the magnitude of service failure, and achieve timely power restoration.

Minimum security standards and mandatory information sharing programs would offer a baseline for aligning the perceptions of disparate industry operators and government agencies regarding the threat landscape and post-disruption objectives. Though the Department of Homeland Security's 2014 NIST Cybersecurity Framework and Voluntary Program could be helpful in reducing organizations' cyber risk, a lack of adoption incentives and concerns about liability have limited its adoption by private infrastructure owners.[25] Shifting the framework from a voluntary program to a set of minimum cybersecurity practices that all owners and operators of critical energy infrastructure must undertake would enhance the resilience of physical systems. Further, an ongoing information-sharing program between private and public stakeholders is needed to ensure private companies have a holistic view of geopolitical cybersecurity trends and threats. Mandating use of cybersecurity sharing programs like the Department of Energy's voluntary CRISP program[26] would provide industry with real-time cyber threat data as well as machine-to-machine threat alerts and mitigation, while alleviating industry concern about sharing trade secrets or revealing cyber weaknesses.

As the shift towards a smart grid expands avenues of attack for malicious actors, incentivizing protective cybersecurity incorporation into smart grid modernizations *before* they are installed will be critical in ensuring cost-efficient resiliency. The Department of Commerce gives several industry-approved options to do so, including collaboration with research and development (R&D) organizations in threat information-sharing programs, exploration of a fast-tracked patent program for infrastructure R&D that has proven to be cybersecure, and engagement with cybersecurity insurance companies to provide risk-based pricing for cybersecurity tools.[27] Further opportunities to incentivize industry cybersecurity include exploring cybersecurity program participation as a criterion for other critical infrastructure grants and even considering technical assistance to the private sector in identifying and/or securing vulnerable components.[28]

The grid's timely recovery from cyberattack will be also be dependent upon a holistic and expansive knowledge of system interdependencies and redundancy measures. As cyberattacks continue to evolve and protective measures against every threat may not be financially feasible, a "50,000-foot view" document identifying every technical component and its purpose, as well as single point of failure components[29] would do well to increase timely recovery. A mandatory document of this sort for every private electric utility would provide anyone in an emergency

with immediate visuals of the system's weak spots to quickly gauge where the problem is coming from and how to fix it.

EMPs Could Cripple Military and Civilian Power for Months

Widespread power outages due to electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) events would result in paralysis of American civilization within seconds, disrupting all technology, access to electricity, water pumps, communication, financial services, transportation, and American offensive and defensive capabilities for months, perhaps years.[30] Although people would not feel the kinetic effects of an EMP from high-altitude nuclear detonation or a GMD caused by a solar flare, the event would likely cause long-term, widespread power outage by permanently debilitating nearly every technological device within the affected vicinity, making the hazard posed by EMP and GMD to the power grid one of the most significant.[31] However, because EMPs and GMDs represent an extremely high-consequence but low-probability event, and because the timing, magnitude, and specific impacts of such an event are difficult to predict,[32] DOE, DHS, and industry have neglected resilience measures against EMPs.[33] Requiring thorough EMP recovery plans and incentivizing investment in EMP-resistant backup energy resources could be the difference between continued societal functioning and a prolonged national tragedy in case of an EMP event.

The Carrington Event of 1859 is the most significant example of a GMD, where an unpredicted solar flare with the energy of 10 billion atomic bombs struck earth, lighting the sky and resulting in technological chaos from America to Europe, with telegraph wires spontaneously bursting into flame and unplugged transmitters continuing to receive input.[34] In Quebec in 1989, a similar GMD occurred at only one-third the strength of the Carrington Event, but cut off power to more than 6 million people in under two minutes,[35] a population similar to that of Tennessee or Arizona.[36] While the probability of an extreme solar storm occurring is relatively low at any given time, it is almost inevitable that one will occur eventually.[37] Historical auroral records suggest a return period of 50 years for Quebec-level storms and 150 years for very extreme storms such as the Carrington Event that occurred nearly 160 years ago.[38]

The national vulnerability to a malicious, man-made EMP is nearly as unpredictable, as there is always a potential for non-state actors and rogue states to gain access to nuclear weapons and ballistic missiles, as well as for states like China and Russia to develop targeted EMP systems like that of the US Air Force CHAMP system (discussed below). Though no actors to date have used an EMP for offensive purposes, the US has demonstrated the technology's ability to take out electricity for large regions as well as single buildings. America first demonstrated the large region effect when it detonated the nuclear weapon "Starfish Prime" above the Pacific Ocean during the Cold War.[39] Though the Starfish Prime test in 1962 was relatively inefficient at producing the EMP effect, it still "fried" nearly all electronic components over 900 miles away from the nuclear explosion,[40] a range that would cover nearly all of the continental US.[41] The US Air Force and Boeing also recently demonstrated a more targeted effect with CHAMP (Counter-electronics High-powered Microwave Advanced Missile Project), a missile system able to plunge single buildings into darkness by pinpointing the electric grid.[42] It is likely that near-peer competitors like China and Russia are developing this technology as well and may find it an

especially appealing weapon for its limited strike zone. If such an event were to occur against the US, most if not all the electric grid's components would be destroyed, and reconstruction would be slow and expensive. The estimated economic disruption of a moderate EMP or GMD is equivalent to more than 20 Katrina-class hurricanes, costing $1 trillion to $2 trillion in the first year and taking more than a decade to recover.[43] Transformers alone—just one component needed for energy distribution—would disrupt parts or all of the grid for 6 months to 2 years because the thousands of transformers on American soil are custom built, imported 85% of the time, cost $2 to $7.5 million apiece, and take 18 to 24 months to manufacture.[44]

Because the threat posed by EMP and GMD is unpredictable, low-probability, and extremely high-consequence, electric utility operators have been unwilling to sufficiently provide for infrastructure resilience. Aligning private industry and government knowledge of the threat and the specific impacts that different EMP waves would have on critical infrastructure will be essential to ensuring that operators know how to move forward in restoring service even when broader technological communications have been disrupted. Though it may not be financially feasible for the federal government to incentivize industry investment in comprehensive mitigation measures, ensuring that grid components in critical areas (military bases, public gathering centers, emergency services, etc.) are EMP resistant would be well worth the relatively miniscule protection costs when compared to the costs of massive life loss and societal panic.

Extreme Weather Event Recovery Dependent Upon Availability of Backup Energy

The rise in frequency and intensity of extreme weather events driven by climate change combined with the current inability of federal and state agencies to restore electricity to affected communities for months on end also demands consideration of more diverse backup energy resources to restore power, safety, and security in the wake of such events. Natural disasters have been responsible for the most widespread and long-term power outages in US history. Further, the number of outages is expected to double every five years because aging infrastructure is unable to cope with more frequent extreme weather and natural disasters.[45]

For example, when Hurricane Maria hit Puerto Rico in 2017, 1.4 million people were left without power for nearly a year because diverse backup generation and transmission systems were not available. In the 2012 Derecho Blackout, a series of thunderstorms, hurricane-force winds, tornadoes, and flash floods resulted in 4.2 million people across 11 states and the District of Columbia losing power for 7-10 days. In the same year, Hurricane Sandy hit New York and New Jersey, depriving millions of power for nearly 2 weeks.[46]

The unpredictability of such events means that simply strengthening existing physical components will not be enough to recover and restore power. Though stockpiling replacements and diverse backups is a pricey proposition for industry members who may see the threat as generally remote, investing in prevention and recovery measures now is likely much cheaper than paying the costs of reputational damage and emergency power restoration. Further, these backups have added value in that they may be sold or transferred to other regions that have been disrupted. Having diverse backup generation, transmission, and distribution devices already manufactured, stored, and readily deployable would be invaluable in restoring power to critical, remote, and highly impacted areas.

Resilient Human Governance: Lack of Incentives, Imagination to Blame for Grid Vulnerability

Resilience of the bulk power system is dependent upon how prepared its human operators are, necessitating **(1)** alignment of private-public objectives and methods for power restoration, **(2)** enhanced incentives for industry to invest in resilience measures, and **(3)** more diverse redundancy measures and backup components. When the market fails to provide users with the information and incentives necessary to prevent the enormous synergistic consequences of grid failure, policy interventions such as these may be necessary.[47]

Existing incentive systems have emphasized common short-term outages but have failed to address high-consequence/low-probability outages, to the detriment of US energy security.[48] Incentives can take several forms, but the most efficacious may be tax incentives and cost-matching with industry to ensure grid modernization efforts are built with security in mind. For example, new components (including distributed SCADA modules, mobile communicators, and embedded control computers) can be EMP-hardened for only 1-3% of the cost of non-hardened items if done at the time of design and manufacturing,[49] whereas retrofitting existing components is drastically more expensive and may only be done for critical system units.[50] Providing financial incentives for demonstrating system resilience may lead to implementation of components inherently able to withstand disruption while nudging industry to address specific system vulnerabilities.[51]

Second, bulk electric system operators should assess the cyber and physical inter-dependencies of their systems in order to address where one component failure could cause broader disruptions. In mapping out critical intersections and windows for cascading failures, officials may be able to install adaptive capabilities like automatic disruption identification and rerouting. In this way, the decentralized and interconnected nature of the electric grid could be advantageous in that multiple points for cyberattack or component failure may also enable multiple points for regaining system control or rerouting energy through other areas.

Resilience Physical Systems: Backup Power Sources Still Vulnerable with Exception of Small Modular Nuclear Reactors

Encouraging the public to develop "homegrown" energy from solar, wind, and diesel generators without a connection to the main grid will remain a valuable source of resiliency, but may provide a false sense of security if such local resources (referred to as distributed energy resources or DERs) are not secure themselves. DERs including solar, wind, combined heat and power, and diesel generators are either unable to provide energy in a longer-term outage or are just as vulnerable to disruption as the main grid. Because of this, serious consideration of Small Modular Nuclear Reactors (SMRs) is merited as a powerful and reliable alternative for building resilience into the US power grid.

While great strides in battery storage have been made, the intermittent nature of solar and wind mean they are still unable to provide the consistent baseload power needed to sustain a community for more than a couple days.[52] Further, the backup power of choice for commercial and private use is emergency diesel generators, which remain vulnerable to cyberattack,[53] EMP and GMD,[54] and supply chain disruptions. Generators run out of gas, and gas stations may be

unable to pump fuel or simply run dry, as occurred during Hurricane Sandy.[55] The federal government maintains a small stockpile of portable generators and fuel, as well as contracts for additional procurements that can be deployed during a major outage, but the quantity available in the event of a large outage is inadequate[56] and the resource's inherent vulnerabilities remain.

Small Modular Nuclear Reactors, like those that power Navy submarines, present a safe, carbon-free, reliable power source able to withstand cyberattack, EMP, and natural disaster like no other resource presently can. A single control room without software operating systems makes SMRs resistant to cyberattack; a faraday cage using metal rods and cement to redistribute electrons makes them EMP/GMD secure; and the design and potential for underground or mobile siting can make them impervious to extreme weather, including Category 1 earthquakes, hurricanes, tsunamis, tornados, fires, and floods. If the main grid and transport infrastructure are disrupted, these generators can support critical facilities for 12 years without a connection to the main grid, without external help to start or shut down, and without refueling.[57]

An analogy used to describe each reactor's size and role is that old nuclear plants are like neighborhoods, while newer SMRs are like mobile homes transported on a semi-truck and left in place, and Micro-Modular Nuclear Reactors (MMRs) have the size and mobility of an RV.[58] Small and Micro-Modular Reactors therefore present a dynamic solution to ensuring energy grid resilience. They are more flexible than other resources in that they are mobile, can swiftly ramp up or down power, and can be grouped together to support different regional needs, with a single module powering a community of over 40,000.[59] Additionally, these generators can be operated by as few as 6 people,[60] take up less than 1/10th of a mile[61] (wind takes 200x as much),[62] can provide heat for water desalination and industrial applications, can be integrated with other DERs, and can be mass produced in factories to make them only slightly more expensive than natural gas and hydroelectricity and cost competitive with fossil fuels and renewables.[63]

As the only energy that provides both 24/7 baseload power like coal and natural gas, and low-carbon energy like solar and wind, while still being resilient to cyber, EMP, and natural disaster, SMRs and MMRs could represent a bipartisan win in ensuring national energy resiliency. Though public opinion polls report that around 50% of Americans support expanding nuclear energy, the divisions in support are not significantly dependent on ideology, gender, or age. Rather, a lack of awareness about modern nuclear technology safety, environmental impacts, and resilience are more likely to account for skepticism where it exists. Decades of public opinion research shows that familiarity with a local nuclear facility, its workers, and economic benefits positively enhances nuclear energy attitudes[64] and reduces risk perceptions.[65] Concerns about energy insecurity and climate change have weaker relationships,[66] suggesting familiarity and trust have greatest impact on attitudes. Because trust plays such a large role in determining nuclear support, and because opinion polls show that 79% of Americans trust the military and scientists to act in the public's interest (far more than elected officials, media, or business leaders),[67] support for modular nuclear reactor pilot programs for military use may enhance civilian support by demonstrating the technology's safety and efficacy while broadening public awareness, familiarity, and comfort with nuclear energy. The support of local environmental groups vouching that the technology is not harmful to local resources or populations would also help alleviate the "not in my backyard" phenomenon associated with the technology.[68]

Though Small and Micro-Modular Nuclear Reactors have significant upfront costs and are still working through advanced development stages—successful demonstration of the technology's resilience at the Idaho National Laboratory will not be completed until 2026[69]—this technology has the potential to dramatically enhance US energy resilience if deployed for use in critical sectors, such as military bases, emergency services and hospitals, and major community centers.

Conclusion

A crisis in the immediate aftermath of a cyberattack, electromagnetic pulse, or extreme weather event is not the time to start planning for systematic recovery of critical infrastructure. As such, the energy industry, Department of Energy, and Department of Homeland Security have a responsibility to ensure plans, resources, and implementation structures are promptly put in place to enhance grid resiliency.[70] Incentivizing **(1)** alignment of stakeholder threat perceptions, infrastructure weaknesses, and recovery objectives, **(2)** protective measures for physical components, and **(3)** more diverse redundancy and backup measures will enable a more resilient grid infrastructure and thus a more resilient society. As such, immediate attention to US grid resilience may be one of America's strongest tools in recovering from cyberattack, EMP, and climate change-driven extreme weather, saving billions of dollars and countless American lives.

Endnotes

[1] Popik, Thomas. n.d. "TESTIMONY OF THE FOUNDATION FOR RESILIENT SOCIETIES." Foundation for Resilient Societies. Accessed April 26, 2019. https://www.ferc.gov/CalendarFiles/20170717080647-Popik,%20Resilient%20Societies.pdf.

[2] Campbell, Richard J. n.d. "The Smart Grid: Status and Outlook." Congressional Research Service. https://fas.org/sgp/crs/misc/R45156.pdf.

[3] Distributed Energy Resources (DERs) are small-scale units of local energy generation connected to the grid at distribution level. They improve cost-efficiency and energy reliability by allowing customers to sell power back to the grid and be compensated for allowing their storage systems to help stabilize the grid, especially during peak periods or times of intermittent supply
"What Are Distributed Energy Resources and How Do They Work? - Australian Renewable Energy Agency." n.d. Accessed April 1, 2019. https://arena.gov.au/blog/distributed-energy-resources/.

[4] "Grid Modernization and the Smart Grid | Department of Energy." n.d. Accessed April 4, 2019. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-Smart-grid.;
Herman K. Trabish, "Smart Inverters: The Secret to Integrating Distributed Energy onto the Grid?," Utility Dive, June 4, 2014, https://www.utilitydive.com/news/Smart-inverters-the-secret-to-integratingdistributed-energy-onto-the-grid/269167/

[5] "DERs Face Increasing Cybersecurity Challenges | Transmission & Distribution World." n.d. Accessed February 22, 2019. https://www.tdworld.com/distribution/ders-face-increasing-cybersecurity-challenges.;
He, H., and J. Yan. 2016. "Cyber-Physical Attacks and Defences in the Smart Grid: A Survey." IET Cyber-Physical Systems: Theory Applications 1 (1): 13–27. https://doi.org/10.1049/iet-cps.2016.0019.

[6] Pandey, Rajendra Kumar, and Mohit Misra. 2016. "Cyber Security Threats — Smart Grid Infrastructure." In 2016 National Power Systems Conference (NPSC), 1–6. Bhubaneswar, India: IEEE. https://doi.org/10.1109/NPSC.2016.7858950.;
R. Anderson and S. Fuloria, "Who controls the off switch?" SmartGridComm, 2010, p 96-101. https://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf ;
P. McDaniel and S. McLaughlin, "Security and privacy challenges in the Smart grid," IEEE Security and Privacy, Vol. 7, No. 3, May/Jun. 2009, pp. 75-77.

[7] Glenn, Colleen, Dane Sterbentz, and Aaron Wright. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," December 20, 2016. https://doi.org/10.2172/1337873.

[8] Pandey, Rajendra Kumar, and Mohit Misra. 2016. "Cyber Security Threats — Smart Grid Infrastructure." In 2016 National Power Systems Conference (NPSC), 1–6. Bhubaneswar, India: IEEE. https://doi.org/10.1109/NPSC.2016.7858950.

[9] Ibid.

10 Glenn, Colleen, Dane Sterbentz, and Aaron Wright. 2016. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." INL/EXT--16-40692, 1337873. https://doi.org/10.2172/1337873.

11 Ibid.

12 "Ukraine's Power Outage Was a Cyber Attack: Ukrenergo - Reuters." n.d. Accessed April 4, 2019. https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.

[13] Glenn, Colleen, Dane Sterbentz, and Aaron Wright. 2016. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." INL/EXT--16-40692, 1337873. https://doi.org/10.2172/1337873.

[14] Sanger, David E. "Russian Hackers Appear to Shift Focus to U.S. Power Grid." The New York Times, October 3, 2018, sec. U.S. https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html.

15 "Russia Considers 'unplugging' from Internet - BBC News." n.d. Accessed April 5, 2019. https://www.bbc.com/news/technology-47198426.

16 Ibid.

17 Glenn, Colleen, Dane Sterbentz, and Aaron Wright. 2016. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." INL/EXT--16-40692, 1337873. https://doi.org/10.2172/1337873.

18 Ibid.

[19] Ibid.

[20] "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps | OPA | Department of Justice." n.d. Accessed April 4, 2019. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.
[21] "What Is Stuxnet, Who Created It and How Does It Work? | CSO Online." n.d. Accessed April 4, 2019. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
[22] Jeannie Johnson with Kerry Kartchner, Marilyn Maines, and Briana D. Bowen. "PASCC Final Report: Assessing Prospects for Iranian Compliance with the JCPOA: An Applied Case Study in Socio-Cultural Modeling and Analysis" (unpublished report for the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction, supported by the United States Air Force Academy and US Department of the Air Force, 2018) 35.
[23] "U.S. Charges Nine Iranians With Cyberattack Campaign." Wall Street Journal. Accessed May 11, 2019. https://www.wsj.com/articles/u-s-charges-nine-iranians-with-cyber-attack-campaign-1521815253.
"U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam." Reuters. Accessed May 11, 2019. https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.
[24] "Iran to Reduce Commitments to Nuclear Deal amid US Pressure, Military Moves - CNNPolitics." Accessed May 11, 2019. https://www.cnn.com/2019/05/07/politics/iran-nuclear-deal-reduce-commitments/index.html.
[25] Jenner, Block LLP-Mary Ellen Callahan, Daniel E. Chudd, and Michael T. Borgia. n.d. "NIST Releases First Cybersecurity Framework, but Questions Remain for Implementation | Lexology." Accessed April 26, 2019. https://www.lexology.com/library/detail.aspx?g=d88db700-2621-4e0f-b6ef-cdb8751237de.
[26] "Energy Sector Cybersecurity Preparedness." n.d. Energy.Gov. Accessed April 26, 2019. https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf.
[27] National Telecommunications and Information Administration. 2013. "Discussion of Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program." 2013. https://www.ntia.doc.gov/report/2013/discussion-and-recommendations-president-incentives-critical-infrastructure-owners-and-o.
[28] Ibid.
[29] Vigeant, Steven. n.d. "How To Find (and Eliminate) Single Points of Failure." Accessed April 26, 2019. https://www.dataev.com/it-experts-blog/how-to-find-and-eliminate-single-points-of-failure.
[30] Foster, Dr John S, Mr Earl Gjelde, Dr William R Graham, Dr Robert J Hermann, Mr Henry, M Kluepfel, GEN Richard L Lawson, Dr Gordon K Soper, Dr Lowell L Wood, and Dr Joan B Woodard. n.d. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," 62. http://www.empcommission.org/docs/empc_exec_rpt.pdf
[31] Campbell, Hershel, and David Stuckenberg. n.d. "Electromagnetic Pulse (EMP) and Space Weather and the Strategic Threat to America's Nuclear Power Stations." Accessed April 4, 2019. http://www.alpf.org/research/emp/.
[32] Chris Neil in an interview with the author. Mr. Neil works national security issues for the FBI and has worked for the DoE on critical infrastructure issues. Phone interview conducted April 24, 2019.
[33] Campbell, Hershel, and David Stuckenberg. n.d. "Electromagnetic Pulse (EMP) and Space Weather and the Strategic Threat to America's Nuclear Power Stations." Accessed April 4, 2019. http://www.alpf.org/research/emp/.
[34] Klein, Christopher. n.d. "A Perfect Solar Superstorm: The 1859 Carrington Event." HISTORY. Accessed April 26, 2019. https://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event.
[35] Zell, Holly. 2015. "The Day the Sun Brought Darkness." NASA. May 13, 2015. http://www.nasa.gov/topics/earth/features/sun_darkness.html.
[36] "List of U.S. States by Population." Wikipedia. Accessed May 11, 2019. https://simple.wikipedia.org/wiki/List_of_U.S._states_by_population.
[37] Campbell, Hershel, and David Stuckenberg. n.d. "Electromagnetic Pulse (EMP) and Space Weather and the Strategic Threat to America's Nuclear Power Stations." Accessed April 4, 2019. http://www.alpf.org/research/emp/.
[38] Ibid.
[39] "The 50th Anniversary of Starfish Prime: The Nuke That Shook the World - Bad Astronomy : Bad Astronomy." n.d. Accessed April 26, 2019. http://blogs.discovermagazine.com/badastronomy/2012/07/09/the-50th-anniversary-of-starfish-prime-the-nuke-that-shook-the-world/#.XMOH0mhKhPY.
[40] "Electromagnetic Pulse - Nuclear EMP - Futurescience.Com." n.d. Accessed April 26, 2019. http://www.futurescience.com/emp.html.

[41] "Draw a Circle with a Radius on a Map." n.d. Accessed April 26, 2019. https://www.mapdevelopers.com/draw-circle-tool.php.
[42] "U.S. Air Force Confirms Boeing's Electromagnetic Pulse Weapon." TRANSCEND MEDIA SERVICE, March 18, 2019. https://www.transcend.org/tms/2019/03/u-s-air-force-confirms-boeings-electromagnetic-pulse-weapon/.
[43] "Catastrophic Power Outages Pose Significant Recovery Challenges." n.d. Accessed April 5, 2019. https://www.govtech.com/em/disaster/US-Recover-Catastrophic-Power-Outage.html.
[44] "Electric Grid Large Power Transformers Take up to 2 Years to Build | Peak Energy & Resources, Climate Change, and the Preservation of Knowledge." n.d. Accessed April 5, 2019. http://energyskeptic.com/2015/power-transformers-that-take-up-to-2-years-to-build/.
[45] "Power Outages On The Rise Across The U.S." n.d. Inside Energy. Accessed March 22, 2019. http://insideenergy.org/2014/08/18/power-outages-on-the-rise-across-the-u-s/.
[46] "9 of the Worst Power Outages in United States History." n.d. Accessed April 5, 2019. https://www.electricchoice.com/blog/worst-power-outages-in-united-states-history/.
[47] "5 Strategies for Reducing the Harmful Consequences from Loss of Grid Power | Enhancing the Resilience of the Nation's Electricity System | The National Academies Press." n.d. Accessed April 4, 2019. https://www.nap.edu/read/24836/chapter/7.
[48] "5 Strategies for Reducing the Harmful Consequences from Loss of Grid Power | Enhancing the Resilience of the Nation's Electricity System | The National Academies Press." n.d. Accessed April 4, 2019. https://www.nap.edu/read/24836/chapter/7.
[49] Foster, Dr John S, Mr Earl Gjelde, Dr William R Graham, Dr Robert J Hermann, Mr Henry, M Kluepfel, GEN Richard L Lawson, Dr Gordon K Soper, Dr Lowell L Wood, and Dr Joan B Woodard. n.d. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," 14.
[50] Ibid.
[51] "The Future of Nuclear Energy in a Carbon-Constrained World." n.d., 275.
[52] "The Future of Nuclear Energy in a Carbon-Constrained World." n.d. MIT Energy Initiative, Future of, , xii.
[53] "Electromagnetic Pulse (EMP) and Space Weather and the Strategic Threat to America's Nuclear Power Stations." n.d. 36. http://www.alpf.org/research/emp/.
[54] Ibid.
[55] "Catastrophic Power Outages Pose Significant Recovery Challenges." n.d. Accessed April 5, 2019. https://www.govtech.com/em/disaster/US-Recover-Catastrophic-Power-Outage.html.
[56] "Catastrophic Power Outages Pose Significant Recovery Challenges." n.d. Accessed April 5, 2019. https://www.govtech.com/em/disaster/US-Recover-Catastrophic-Power-Outage.html.
[57] Conca, James. n.d. "NuScale's Small Modular Nuclear Reactor -- Reliable, Resilient and Flexible." Forbes. Accessed February 27, 2019. https://www.forbes.com/sites/jamesconca/2018/06/22/nuscales-small-modular-nuclear-reactor-reliable-resilient-and-flexible/.
[58] Author interview of retired Lt. Col. Kenneth Allen of West Point Military Academy, 20 March 2019.
[59] Conca, James. n.d. "NuScale's Small Modular Nuclear Reactor -- Reliable, Resilient and Flexible." Forbes. Accessed February 27, 2019. https://www.forbes.com/sites/jamesconca/2018/06/22/nuscales-small-modular-nuclear-reactor-reliable-resilient-and-flexible/. ;
"The NuScale SMR: Now Nuclear Goes 'Off the Grid.'" n.d. Accessed April 4, 2019. https://www.nei.org/news/2018/nuscale-smr-now-nuclear-goes-off-grid.
[60] ChoFeb. 21, Adrian, 2019, and 8:00 Am. 2019. "Smaller, Safer, Cheaper: One Company Aims to Reinvent the Nuclear Reactor and Save a Warming Planet." Science | AAAS. February 19, 2019. https://www.sciencemag.org/news/2019/02/smaller-safer-cheaper-one-company-aims-reinvent-nuclear-reactor-and-save-warming-planet.
[61] "SMRs-A-Different-Approach_WP.Pdf." n.d. Accessed March 8, 2019. https://www.hl.com/uploadedFiles/11_Blogs/Strategic-Consulting/SMRs-A-Different-Approach_WP.pdf.
[62] Ibid.
[63] Conca, James. n.d. "NuScale's Small Modular Nuclear Reactor Passes Biggest Hurdle Yet." Forbes. Accessed February 25, 2019. https://www.forbes.com/sites/jamesconca/2018/05/15/nuscales-small-modular-nuclear-reactor-passes-biggest-hurdle-yet/.;

Cho, Adrian. "Smaller, Safer, Cheaper: One Company Aims to Reinvent the Nuclear Reactor and Save a Warming Planet." Science | AAAS. February 19, 2019. https://www.sciencemag.org/news/2019/02/smaller-safer-cheaper-one-company-aims-reinvent-nuclear-reactor-and-save-warming-planet.

[64] J. Baxter, D. Lee "Understanding expressed low concern and latent concern near a hazardous waste treatment facility" Journal of Risk Research, 7 (7) (2004), pp. 705-729;
K. Burningham, D. Thrush, "Pollution concerns in context: a comparison of local perceptions of the risks associated with living close to a road and a chemical factory," Journal of Risk Research, 7 (2) (2004), pp. 213-232;
A. Blowers, P. Leroy "Power, politics and environmental inequality: A theoretical and empirical analysis of the process of peripheralization," Environmental Politics, 3 (2) (1994), pp. 197-228;
W. Freudenberg, D. Davidson, "Nuclear families and nuclear risk: The effects of gender, geography and progeny on attitudes towards a nuclear waste facility," Rural Sociology, 72 (2) (2007), pp. 215-243;
M.R. Greenberg, "NIMBY, CLAMP, and the location of new nuclear-related facilities: USA national and 11 site-specific surveys," Risk Analysis, 29 (9) (2009), pp. 1242-1254;
G. Hecht, "The radiance of France: Nuclear power and national identity after World War II," MIT Press, Cambridge, MA (1998);
Parkhill et al, "From the familiar to the extraordinary: Local residents' perceptions of risk when living with nuclear power in the UK," Transactions of the Institute of British Geographers, 35 (1) (2010), pp. 39-58

[65] L. Sjöberg, B.M. Drottz-Sjöberg, "Knowledge and risk perception among nuclear power plant employees Risk Analysis," 11 (4) (1991), pp. 607-618.

[66] Corner, Adam, Dan Venables, Alexa Spence, Wouter Poortinga, Christina Demski, and Nick Pidgeon. 2011. "Nuclear Power, Climate Change and Energy Security: Exploring British Public Attitudes." Energy Policy 39 (9):4823–33. https://doi.org/10.1016/j.enpol.2011.06.037.

[67] "Most Americans Trust Military, Scientists to Act in Public Interest." n.d. Accessed April 6, 2019. https://www.pewresearch.org/fact-tank/2016/10/18/most-americans-trust-the-military-and-scientists-to-act-in-the-publics-interest/.

[68] Chris Neil in an interview with the author. Mr. Neil works national security issues for the FBI and has worked for the DoE on critical infrastructure issues. Phone interview conducted April 24, 2019.

[69] "5 Nuclear Storylines to Watch for in 2019," Department of Energy. Accessed May 11, 2019. https://www.energy.gov/ne/articles/5-nuclear-storylines-watch-2019.

[70] Chris Neil in an interview with the author. Mr. Neil works national security issues for the FBI and has worked for the DOE on critical infrastructure issues. Phone interview conducted April 24, 2019.