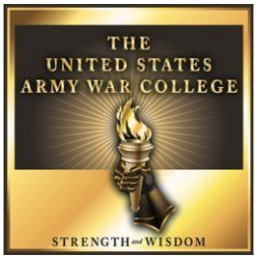
Strategy Research Project

Strategic Implications of a Vulnerable Electric Power Grid

by

Lieutenant Colonel James D. Willson
United States Army National Guard



United States Army War College
Class of 2015

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2015	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Strategic Implications of a Vulnerable Electric Power Grid

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel James D. Willson
United States Army National Guard

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Matthew Molineux
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5011

14. ABSTRACT

Electricity is the lifeblood of our economy and the assumption of near continuous flow is taken for granted because the industry has achieved a remarkable level of reliability. But market pressure to find efficiencies coupled with weak government oversight is making the grid and society more vulnerable to the consequences of long-term power failures than they should be. At the direction of Congress, the Department of Defense is taking steps to isolate military installations from the commercial power grid to protect the capability to project military power. But increasing vulnerabilities to blended cyber and physical attacks could force the Department to deal with the consequences of large scale civil unrest and chaos domestically. Just as the Federal Aviation Administration regulates nearly all aspects of the aviation industry to counter the temptation to increase profits at the expense of public safety, the Department of Energy should regulate the power utilities similarly to ensure baseline reliability. However, long-term reliability will be achieved when renewable energy micro-grids are installed in thousands of communities and networked together similar to the internet in terms of scope, scale and reliability.

15. SUBJECT TERMS
Solar, NRC, FERC, Policy, DOE, Cyber, Blackout, DCIP, CIP, Infrastructure, Wind

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	30	

USAWC STRATEGY RESEARCH PROJECT

Strategic Implications of a Vulnerable Electric Power Grid

by

Lieutenant Colonel James D. Willson
United States Army National Guard

Colonel Matthew Molineux
Department of National Security and Strategy
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Strategic Implications of a Vulnerable Electric Power Grid

Report Date: 01 April 2015

Page Count: 30

Word Count: 5011

Key Terms: Solar, NRC, FERC, Policy, DOE, Cyber, Blackout, DCIP, CIP, Infrastructure, Wind

Classification: Unclassified

Electricity is the lifeblood of our economy and the assumption of near continuous flow is taken for granted because the industry has achieved a remarkable level of reliability. But market pressure to find efficiencies coupled with weak government oversight is making the grid and society more vulnerable to the consequences of long-term power failures than they should be. At the direction of Congress, the Department of Defense is taking steps to isolate military installations from the commercial power grid to protect the capability to project military power. But increasing vulnerabilities to blended cyber and physical attacks could force the Department to deal with the consequences of large scale civil unrest and chaos domestically. Just as the Federal Aviation Administration regulates nearly all aspects of the aviation industry to counter the temptation to increase profits at the expense of public safety, the Department of Energy should regulate the power utilities similarly to ensure baseline reliability. However, long-term reliability will be achieved when renewable energy micro-grids are installed in thousands of communities and networked together similar to the internet in terms of scope, scale and reliability.

Strategic Implications of a Vulnerable Electric Power Grid

> For as long as anyone can remember, reliable, cheap electricity has been taken for granted in the United States.
>
> —Alex Berenson[1]

The economy is the ultimate source of U.S. national power. Extraordinary economic success since the early twentieth century enabled substantial investments in military technology, diplomatic capital and national infrastructure that made the U.S. the powerhouse it is today. Abundant natural resources available to people governed by a liberal democracy organized by capitalism sparked the first industrial revolution, but it was the electrification of the U.S. that literally powered the second industrial revolution and paved the way for extraordinary economic prosperity.

Commercial electrification began on August 26, 1895, in Niagara Falls, New York, when some water flowing over the falls was diverted through a pair of turbines. One year later, 11,000 volts of electricity was transmitted twenty miles by wire to Buffalo, New York, where it was used for lighting and powering street cars.[2] From this modest beginning, sprang the complex electric power grid that we have today. According to a report published by the U.S. House of Representatives Committee on Commerce and Energy, “The U.S. bulk-power system serves more than 300 million people and is made up of more than 200,000 miles of transmission lines, and more than 1 million megawatts of generating capacity, and is valued at over $1 trillion.” [3] This paper will argue that electric power is the lifeblood of the U.S. economy and the assumption of near continuous flow underpins all instruments of national power, but a confluence of factors such as weak government oversight, centralized design

architecture and societal dependency, is making the U.S. more vulnerable to long-term power outages than it should be.

Figure 1: New York ca.1880 illuminated by Brush electric arc-lamps[4]

This vulnerability exists at a time when sophisticated adversaries are testing the boundaries of cyber warfare by targeting critical infrastructure and defense networks on a continuous basis.[5] However, recent Congressional actions taken to improve electric reliability only on military bases suggest an under-appreciation for the substantial military commitment that would be needed to deal with a long-term outage on the civilian grid. The demand for domestic military manpower could be a significant distraction for the Department of Defense (DOD) as it struggles to assist overwhelmed local authorities faced with widespread civil unrest and chaos at a time that may signal the start of hostilities elsewhere in the world. Better government regulation and strong incentives to foster the adoption of locally generated renewable electricity could virtually eliminate the threat of widespread blackouts, safeguard the economy and protect all instruments of national power.

DOD and Commercial Power

The purpose of DOD installations is to, “Sustain the regular forward and home station presence of U.S. forces as well as provide support in training and deployment to meet the Nation’s need in periods of crisis, contingency, and combat.”[6] In order to provide a reasonable level of assurance that a facility can accomplish its missions, base officials must identify essential functions and apply resources to mitigate risks of partial or total loss of the functions. Electric power supports almost all base functions and DOD installations derive almost all of their electric power from commercial utility providers. “About 85% of the energy infrastructure upon which DOD depends is commercially owned, and 99% of the electrical energy DOD installations consume originates outside the fence.”[7] To mitigate the risk of an interruption in the commercial power supply, installation managers rely on small diesel generators with short-term fuel supplies in most cases. When facilities have substantial Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and military strategic deterrence missions, base officials typically invest in larger diesel powered backup generators to mitigate the risk of a power loss.[8] But according to a report by the Defense Science Board (DSB) in 2008, “Backup power systems at these installations are larger, but are still based on diesel generators and fuel supplies sized for only short-term commercial outages and seldom properly prioritized to critical loads because those are often not wired separately from non-essential loads.”[9] The same report also challenged the prevailing assumption that future power-outages will continue to be short lived and relatively rare occurrences.

Long-term in the context of a power-outage is not precisely defined in Defense Critical Infrastructure (DCI) protection guidance. This means that managers of DCI have

little incentive to expend resources to mitigate the risk of a loss of commercial power for longer than a few days. In a General Accounting Office (GAO) report published in 2009 on DCI, one recommendation encouraged DOD to, "develop explicit Defense Critical Infrastructure Program guidelines for assessing the critical assets' vulnerabilities to long-term electrical power distributions."[10] While the official DOD response to GAO's finding was concurrence, the Office of the Secretary of Defense (OSD) noted, "25 of the 34 assets surveyed reported that electrical power disruptions resulted in no or minimal impact to their missions. The department is working on providing the same protection from commercial power disruption to the remaining assets."[11] OSD's response suggested some resistance to GAO's assertion that backup power systems should be able to cope with extended outages longer than a few days. But two years later, the National Defense Authorization Act (NDAA) of 2010 put new emphasis on energy assurance for DOD installations by introducing the concept of *islanding* to reduce reliance on commercial power providers.

The term islanding refers to the condition in which a power generation source continues to power a location even though electric grid power from the electric utility is no longer present.[12] To that end, the NDAA 2010 directed a study to, "assess the feasibility of developing nuclear power plants on military installations."[13] While the purpose of islanding installations is strait forward, the strategic implications are less clear. According to one strategic forum's paper published by National Defense University in 2011, "Making bases more resilient to civilian power outages would reduce the incentive for an opponent to attack the grid. An opponent might still attempt to take

down the grid for the sake of disrupting civilian systems, but the powerful incentive to do so in order to win an ongoing battle or war would be greatly reduced."[14]

However, disruption of the civilian power grid could be far more effective at disrupting DOD operations if the outage was widespread and long in duration. According to a report on the vulnerability of the power grid produced by the Department of Energy (DOE) in 2009, "In addition to the immediate loss of lighting and electric appliances in the affected area, the supply of food, water and fuel would degrade within days. After several days, widespread social unrest and confusion would ensue."[15] Social unrest and confusion could quickly overwhelm local officials and require extensive domestic assistance from military forces in the form of manpower and equipment.

Without electric power, basic services and safeguards begin to degrade immediately. When the lights go out, some people will take advantage of the rare opportunities to loot businesses and set a fire which is exactly what happened in July 1977, in New York after only about 36 hours without electric power. In a short period of time, 1,616 businesses were looted, 3,900 fires were set and approximately 3,400 people were arrested.[16] Social order broke down quickly and police and fire departments were completely overwhelmed. While the short duration of the blackout in New York obviated the need for federal or National Guard forces to help restore order, it is easy to imagine similar scenarios playing out in a country that has only grown more dependent on electrical power in the intervening years since 1977. An attack on the power grid is a real threat that can be accomplished by a dedicated adversary with modest means and little fear of getting caught. While there is increasing public

awareness of grid vulnerability, Congress has demonstrated reluctance to exert power over private utility companies to require improvements in reliability standards.[17] This reluctance illustrates the inherent tension that can exist when critical infrastructure is owned and operated by powerful private companies.

Competing Interests

Until 2005, reliability standards for the nation's electric power grid were left entirely in the hands of the power industry. According to the DOE, "Investor-owned utilities account for ownership of over 50% of net generation and almost 80% of transmission."[18] The transmission part means that most of the bulk power system that moves electricity from generation plants to consumers is privately owned and operated. Private ownership of the grid has served the public well as evident by the remarkably reliable and efficient industry we have today. But private owners are motivated to improve shareholder value by maximizing profit, so utility companies have powerful incentives to find and implement cost cutting efficiencies wherever they can. This behavior is rational and expected by the shareholders who expect returns on their investments. Over the years, managers and owners of the bulk power transmission network have found creative ways to reduce costs by eliminating redundancies and investing in automated switching technologies which has resulted in a lean bulk power distribution network with fewer pathways for electricity to be routed around trouble spots.[19]

The tradeoff between efficiency and reliability was highlighted on August 14, 2003, when a sagging power line in Ohio contacted a tree and triggered a cascading series of events which led to one of the most widespread blackouts in U.S. history.[20] In the northeastern U.S. and Canada, approximately 55 million people were affected by a

power blackout that lasted two days in some places.[21] The cause of the interruption was attributed to a combination of equipment failures and human error but the real cause was rooted in week governance because compliance with grid-reliability rules was voluntary at the time. According to Mike Jacobs, a senior energy analyst, “The 2003 blackout had many lessons, but for the industry and regulators, the big one was: Make the grid reliability rules mandatory and enforceable!”[22] In contrast to 1977, however, the 2003 blackout did not trigger civil unrest, but that reality may be attributable to a polarizing event which took place in the same region less than two years earlier--the terrorist attacks of September 11, 2001 (9/11). The close proximity in time and location to 9/11, coupled with the short duration of the blackout, may have averted a civil crisis; but the tension between efficiency and reliability still exists today despite the criticality of the power grid to our economic prosperity and national security.

The North American Electric Reliability Corporation (NERC) is the not-for-profit international regulatory authority charged with developing and enforcing reliability standards for bulk power distribution between Canada, U.S. and portions of northern Mexico. NERC divides the components of the electric power grid into two main categories--the bulk power system and local distribution network. It is the bulk power system that is most vulnerable to attack because that is where electricity is most concentrated and the pathways are least redundant as power is collected from power plants and transmitted long distances to local distribution networks. According to NERC, “The North American bulk power distribution system consists of over 200,000 miles of high-voltage transmission lines, thousands of generation plants, and millions of digital controls. More than 1,800 entities own and operate portions of the systems, with

thousands more involved in the operation and distribution networks across North America."[23] It is the bulk power system that interconnects the utility companies with the local users and it is the system that is most fragile and vulnerable to a range of threats including coordinated physical and cyber-attacks.

Alarmed by the demonstrated fragility of the power grid after the 2003 northeast blackout, Congress passed the Energy Policy Act (EPAct) of 2005 which gave FERC more authority to impose reliability standards on owners and operators of the grid. The legislation gave FERC new authorities to appoint an Electric Reliability Organization (ERO) to develop and propose mandatory reliability standards for all owners, users and operators of the bulk power system.[24] In accordance with EPAct, FERC tasked NERC to set reliability standards for the industry enforceable by fines beginning in 2006. However, according to the Defense Science Board (DSB) and others, "NERC is a voluntary private industry coordinating body whose members come mostly from the power industry--the very industry that they are charged to make more reliable and resilient."[25]

A potential conflict of interest exists between the power industry, a rule making body that is dominated by the industry they regulate, and the need to protect our most critical infrastructure from serious threats. As the DSB noted, "While the regulatory structure created by EPAct 2005 is an improvement, it is not the same as government authority to directly establish and enforce reliability standards."[26] From the perspective of utility company owners, risk mitigation investment strategies like hardening substation facilities, developing strong encrypted system control software, and stockpiling custom made transformers are costs that are difficult to pass on to customers. This weak

enforcement and economic incentive structure is one reason the power grid is not as secure as it could be, and our instruments of national power are more vulnerable than they should be.

Vulnerability of the Grid

There is evidence that electric grid infrastructure is being tested by adversaries now. In April 2013, a small substation outside of San Jose, California, was attacked by several gunmen who fired on seventeen large transformers over a period of 19 minutes while successfully evading police.[27] While the utility company managed to route electric power around the site in time to avert an outage, the effects would have been far worse if another interconnected substation was targeted simultaneously in a coordinated way or if digital switching components were compromised to induce cascading failures. After the San Jose gunfire incident, NERC proposed and passed rules that sounded like they were intended to harden key substations from similar attacks, but as the *Wall Street Journal* pointed out, "draft regulations—written by the power industry—are drawing criticism from experts who say the proposals are too loose to stop saboteurs. Among other things, the rules would allow electric companies to decide for themselves what threats are realistic and what steps to take to safeguard equipment."[28]

According to DOE, "The risk of a coordinated cyber, physical, or blended attacks against the North American bulk power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to be reduced."[29] High voltage transformers are perhaps the most vulnerable and difficult components of the bulk power system to protect because they carry so much electricity. Destruction of transformers can seriously

reduce the transmission capacity of a regional electric power grid and lead to extended blackouts.[30] They are unique and built to custom specifications for each site with a manufacturing lead time between 5 to12 months but foreign built models can take as long as 20 months for delivery.[31] High voltage transformers are expensive and highly reliable under normal conditions so utility companies have little incentive to purchase spares for the unlikely event of failure under normal conditions. According to DOE, "the factory prices for transformers typically range from $2 million for a 230 kV unit to $7.5 million for a 765 kV unit, before transportation and installation costs."[32] The combination of high reliability, high replacement cost and custom manufacturing means there is little incentive for utility companies to stockpile spare transformer parts in large numbers which makes long-term power outages more likely in the event of a deliberate coordinated attack on substations.

A coordinated attack on the bulk power system by a knowledgeable adversary would be relatively easy to commit and could be highly effective. In many cases, high powered rifles fired from outside a transformer site would be enough to completely destroy a one-of-a-kind key transformer. While electricity could be routed effectively around one or two damaged or destroyed sites, the network begins to fail in cascading ways when several key components are destroyed in close succession. According to the Office of Technology Assessment, "Some of these components are vulnerable to saboteurs with explosives or just high-power rifles. Not only would repairs cost many millions of dollars, but the economic and societal damage from serious power shortages would be enormous."[33] The same report also noted that design elements of bulk power systems are universal around the world so foreign adversaries would not have to travel

to study the theoretical vulnerabilities of the bulk power system in North America. In March 2014, *the Wall Street Journal* (WSJ) reported that an unreleased study by the Federal Energy Regulatory Commission (FERC) states that nine of the North America's 55,000 substations could cause a coast-to-coast blackout for at least 18 months if successfully attacked.[34] The report quoted a memo prepared for FERC chairman Jon Wellinghoff, "Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer."[35]

In addition to physical attacks on key nodes sophisticated adversaries could create synergistic effects delivered through cyber systems. DOE pointed out in 2009, "A highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes."[36] Proliferation of Smart Grid technology and computer controlled switches also creates opportunity for nefarious actors to interrupt automated processes designed to enhance grid reliability and efficiency. Cyber delivered attacks, coupled with discrete stand-off physical attacks with high powered rifles and explosives have the added benefit of being difficult to assign blame. The potential for high societal impacts, ambiguous attribution and military distraction makes the civilian electric power grid an especially attractive target. An enemy with a few knowledgeable agents could perpetrate an attack designed to degrade the economy, distract the military, confuse public opinion and erode virtually all instruments of national power in a very short period of time with only a small investment in manpower and material.

Long-term Power Outage

According to Army Techniques Publication 3-39.33, *Civil Disturbances*, "When authorized by the Secretary of Defense, federal military forces may provide indirect support to law enforcement agencies; but support is limited to logistical, transportation, and training assistance except when emergency authority applies. State and territorial governors can use state National Guard forces for direct support to civilian law enforcement; however, such use is a temporary expedient and must be in accordance with state laws."[37] Civil unrest during a widespread and long-term power outage is likely given North America's deep dependence on electric power. Table 1 highlights some of the main effects power outages have on various sectors of society.

Table 1: Sector Impacts of Power Loss[38]

Sector	Impacts	Effects
Industrial	Highly sensitive	Spoilage of raw materials Lost productivity
Transportation	Virtually Every Mode	Subways; elevators; street lights; gasoline pumps; airports in emergency mode; trains can move but dangerous.
Telecommunications	Highly Sensitive	Telephone backup generation approximately 7 days; Internet outage
Emergency Services	Highly Sensitive	Firefighting and Police disrupted by high volume; confusion
Public Utilities	Highly Sensitive	Gravity fed water pressure can last 24 hours; Sewage treatment stops; Loss of water pressure hampers firefighting
Banking	Highly Sensitive	Heavily computer-dependent; electronic transactions degraded
Residential	Highly Sensitive	Lights, refrigerators and freezers, stoves and microwave ovens, toasters, dishwashers, intercoms, televisions, clocks, computers, doorbells, hair dryers, heated blankets, can openers, food

		processors, carving knives, toothbrushes, razors, and garage door openers.

Over time, electricity has transformed from a convenience to a necessity and utility companies have responded to demand with prudent investments in the bulk power system to make the grid reliable and safe for customers. However, deepening reliance on electricity has made society profoundly vulnerable to an outage and that reality should prompt us to challenge our assumptions about how to protect the grid.

What if a blackout was widespread throughout the northeast U.S. and the duration was measured in weeks or even months? How would the average person obtain food and clean water when automated bank teller machines do not work and physical banks do not have enough resources on hand to satisfy sudden demands for cash? How long will social order last when millions are faced with this reality after backup generators begin to run out of fuel? Finally, what will happen when all of this occurs as a precursor for an attack on our interests abroad while thousands of state and federal forces are busy supporting law enforcement agencies and distributing emergency commodities like food and water to millions of affected people?

An attack on the electric grid that caused widespread outages would be regarded as an outrageous act of aggression by the public which would likely strengthen public resolve for swift attribution. While military theorists in the interwar period of the early 20th century, predicted people subjected to the horrors of strategic bombing would quickly give up and sue their governments to make peace, in reality, such tactics only served to strengthen public resolve and enmity.[39] Affected citizens would be more likely to endure hardships during a blackout in a cooperative and civilized way if responsibility

could clearly be assigned to a perpetrator. But the asymmetry of a blended cyber and clandestine physical attack on a few key nodes in the bulk power system could effectively obfuscate the source of the attack and make it difficult or impossible to assign attribution in a clear way that would strengthen resolve and avert public unrest. The 2014 Quadrennial Defense Review highlighted the environment succinctly, "Further, potential adversaries are actively probing critical infrastructure throughout the United States and in partner countries, which could inflict significant damage to the global economy and create or exacerbate instability in the security environment."[40]

Theory

According to Joint Doctrine and numerous policy documents, national power is comprised of multiple and overlapping sources or *instruments*; DIME (Diplomatic, Informational, Military and Economic Power). [41] Statesmen are charged with orchestrating and wielding power to achieve broad goals and objectives such as national sovereignty and economic prosperity. While the DIME instruments each have complex and diverse sources of internal power, one aspect is common to each--the health of the national economy. According to Joseph Nye, "Military force has been called "the ultimate form of power" in world politics, but a thriving economy is necessary to produce such power."[42] Nye pointed out in his book, The *Future of Power*, "Although the cultural and social problems discussed thus far do not seem likely to weaken American power, failure in the performance of the American economy would be a real show stopper."[43] The same is true for the diplomatic, informational and economic instruments of power because they ultimately draw their strength from the economy. A former Central Intelligence Agency official, Ray Cline, attempted to quantify perceived national power in 1977 with the equation: Perceived Power= (Population + Territory +

Economy + Military) X (Strategy + Will).[44] Using this expression, Cline calculated the Soviet Union to be twice as powerful as the U.S.. But in 1991, the Soviet Union collapsed largely because of economic stress created by the Cold War induced arms race.[45] While there is no way to prove Cline's equation, historical results suggest that the variable *economy* should have been multiplied by a constant or raised by an exponent to better express its importance in estimating perceived national power.

Nye continues to describe two broad power shifts at play in contemporary international relations, "Two great shifts are occurring in this century: a power transition among states and a power diffusion away from all states to non-state actors."[46] This shift makes soft targets such the electric power grid attractive due to the potential effects on military forces needed to help with internal security and relief efforts, and the indirect effects caused by a sudden stop of the economy. Rival nations, sensing opportunities to improve their status by weakening U.S. power, could be emboldened to launch clandestine blended attacks on the U.S. power grid as a precursor to challenges to our security commitments elsewhere in the world. Finally, non-state actors intent on inflicting as much suffering as possible would likewise find the power grid equally attractive for its acute vulnerability to widely available conventional weapons and cyber systems coupled with the potential for catastrophic effects.

Recommendations

It is time for direct federal oversight of the bulk power distribution system by DOE. Rulemaking bodies like NERC are too close to the industry they are supposed to regulate and the conflict of interest makes them less effective. In 2014, the 113th Congress introduced but failed to pass the Grid Reliability and Infrastructure Defense Act that would have given NERC even more authority to enforce reliability standards,

but the bill failed in the face of strong industry opposition.[47] Congress' sense of urgency to fully empower the regulatory bodies responsible for the reliability standards does not match the severity of the situation. The Federal Aviation Administration, for example, regulates nearly every aspect of safety in the airline industry from pilot training and rest rules to airplane maintenance standards.[48] This level of oversight is necessary for an industry driven by market forces where the consequence of failure is high. The societal cost of a widespread power failure could be catastrophic and provide a significant distraction for DOD at a time when security interests are threatened at home or abroad.

Islanding DOD installations is a good start and it highlights another mitigation strategy that should be accelerated through legislation--localized solar and wind power generation. The more power that can be generated locally, the less reliant we would be on centralized bulk power distribution systems which are vulnerable to attack. The technology exists today to drastically reduce reliance on fossil fuel and long distance power transformation. According to the National Renewable Energy Laboratory, "If all of the residential and commercial rooftops were covered with solar panels, the U.S. could produce 819 TW-hr of electricity, or about 22% of what is consumed each year."[49] That capacity assumes existing solar technology, but technology is improving the efficiency of solar panels at an exponential rate. A nation covered in rooftop solar panels would be virtually impervious to blackouts and the enhanced reliability would safeguard our economy and preserve military power for more appropriate use.

In India, July 2012, the world got a glimpse of how solar powered micro-grids can insulate people from the risks associated with centralized power generation and long distance distribution. While more than 700 million people were affected by a blackout

that darkened 20 of India's 28 states, the remote village of Meerwanda was completely unaffected because of an experiment conducted by the U.S. based solar energy company SunEdision. According to Reuters, "Meerwada, on a dirt track rutted by rains and outside the reach of the national grid, struck lucky when U.S. solar firm SunEdison picked it to test out business models and covered the hefty initial expense of installing hi-tech solar panels in the heart of the village."[50] Meerwanda showed that localizing power generation with renewable resources like solar and wind can nearly eliminate the possibility of wide scale blackouts. This model of localized power generation would create a mesh-network similar to the internet in scale and reliability that offers the best chance to mitigate the risks inherent in the centralized generation and distribution model for electricity we have today. Author Jeremy Rifkin explains, "Unfortunately, the United States is playing directly into the hands of cyber-terrorists by championing a centralized smart grid. The European Union and other governments, by contrast, are deploying a distributed smart grid--or Energy Internet--that lessens the potential threat and damage that can be inflicted by massive cyber-attack."[51]

Conclusion

The bulk power system in North America is a complex critical infrastructure that has gradually become more than a convenience for modern life. Virtually every sector of society depends on near continuous flow of power and DOD is no exception. While mitigation strategies such as islanding of DCI to guard against the potential of long-term outages is prudent, the reliability of the rest of the commercial power grid should not be left to market forces alone. If left under-protected and vulnerable, state and non-state actors could take advantage of our precarious dependency on centralized electric power

generation and distribution by perpetrating blended attacks designed to conceal the attackers and cause massive power outages over large areas. Widespread blackouts lasting weeks or months inflicted by anonymous assailants could result in public confusion and increases the chances for civil unrest and chaos on an unimaginable scale. A widespread blackout would require DOD help from federal and National Guard forces to both assist police in quelling civil unrest and other civil authorities in the distribution of basic commodities like food and water with transportation assets. This enormous demand for DOD forces would seriously distract and undermine our military instrument of national power despite having invested in power islanding strategies such as small nuclear reactors on DOD installations.

Congress should mandate federal oversight of the electric utility industry similar to the way the Federal Aviation Administration oversees the airline industry. Both industries are privately owned critical infrastructure subject to market forces which gives managers powerful incentive to cut costs and increase efficiency. If left vulnerable, our enemies have strong incentives to target both. The U.S. learned after 9/11 that passenger screening could no longer be left to the individual airline companies, but we had to pay a terrible price for that lesson. The cost is simply too great to learn a similar lesson after the power goes out and society begins to dissolve along with our combat power and economy.

Federal oversight of the existing model of centralized power generation and long distance bulk distribution is only the first step. Government should continue to incentivize the investment and development of locally-generated renewable energy such as solar and wind power. Decentralizing the national power grid in favor of

renewable micro-grids would not only reduce carbon emissions, it will protect our economy--our fundamental source of national power.

Endnotes

[1] Alex Berenson, “Ideas & Trends; Power: Get It While It Lasts,” *New York Times,* August 2000, http://www.nytimes.com/2000/08/06/weekinreview/ideas-trends-power-get-it-while-it-lasts.html (accessed December 10, 2014).

[2] Smithsonian Institution. “Origin of Electrical Power.” *Powering a Generation of Change* (Washington DC: Smithsonian Institution, 2014), 1.

[3] Edward J. Markey and Henry A Waxman. *Electric Grid Vulnerability: Industry Response Reveals Security Gaps.* Congressional, Washington DC: Congressional Staff, 2013, 4.

[4] Smithsonian Institution. “Origin of Electrical Power.” *Powering a Generation of Change* (Washington DC: Smithsonian Institution, 2014), 1.

[5] Steve Reilly. "Bracing for a big power grid attack: 'One is too many'." *USA Today.* March 24, 2015. http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/ (accessed March 26, 2015), 1.

[6] Office of the Secretary of Defense (Installations and Enviornment). *2007 Defense Installations Strategic Plan.* Washington , DC, 2007, 3.

[7] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. 2008. Independent Federal Advisory Committee Report, Washington DC: Department of Defense, Report of the Defense Science Board Task Force on DOD Energy Strategy: “More Fight-Less Fuel”, 21.

[8] Ibid., 53

[9] Ibid.

[10] Government Accountability Office. *Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets.* Congressional Report, Washington: United States Government Accountability Office, 2009, 78.

[11] Ibid.,78.

[12] Chris Greacen, Richard Engel, and Thomas Quetchenbach. "A Guidebook on Grid Interconnection and Islanded Operation of Mini-Grid Power Systems Up to 200 kW." Guidebook. Berkeley: Lawrence Berkeley National Laboratory, April 1, 2013, 12.

[13] 111th Congress. *National Defense Authorization Act for Fiscal Year 2010.* Public Law 111-84, Washington DC: Government Printing Office, 2010, SEC. 2845.

[14] Richard B.Andres and Hannah L Breetz. *Small Nuclear Reactors for Military Installations: Capabilities, Costs, and Technological Implications.* Strategic Forum, Washington DC: Institute of Strategic Studies, 2011, 4.

[15] North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* Report, Washington DC: Department of Energy, 2009, 21.

[16] Robert Curvin and Bruce Porter. *Blackout Looting!* (New York: Gardner Press), 1979, 3-5.

[17] Timothy Cama. "Bill would give feds new power to protect electric grid." *The Hill*. March 26, 2014. http://thehill.com/policy/energy-environment/201834-bill-would-give-feds-new-power-to-protect-electric-grid (accessed March 26, 2015).

[18] Department of Energy. Electricity 101. January 29, 2014. http://energy.gov/oe/information-center/educational-resources/electricity-101#ppl1 (accessed January 29, 2014).

[19] Battelle Memorial Institute. *Recommendations for Implementing Comprehensive Bulk-Power System Security Standards.* White Paper, Columbus: Battelle Memorial Institute, 2014, 1.

[20] The History Channel. Blackout: The Worst Power Outages in History. August 14, 2013. http://www.history.com/news/blackout-the-worst-power-outages-in-history (accessed January 13, 2015).

[21] CNN. Major Power Outage hits New York, other large cities. August 14, 2003. http://www.cnn.com/2003/US/08/14/power.outage/ (accessed January 31, 2015).

[22] Mike Jacobs. "Not a Good Day in the Neighborhood"--Electricity Grid Progress since the August 2003 Blackout. August 12, 2013. http://blog.ucsusa.org/electricity-grid-progress-since-the-august-2003-blackout-202 (accessed February 1, 2015).

[23] Ibid., 23.

[24] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. 2008*. Independent Federal Advisory Committee Report, Washington DC: Department of Defense, Report of the Defense Science Board Task Force on DOD Energy Strategy: "More Fight-Less Fuel*", 56.

[25] Ibid., 56.

[26] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. 2008. *Independent Federal Advisory Committee Report, Washington DC: Department of Defense, Report of the Defense Science Board Task Force on DOD Energy Strategy: "More Fight-Less Fuel"*, 57.

[27] Ibid., 1.

[28] Rebecca Smith. “Proposal to Prevent Grid Attack Lacks Power, Critics Say”, *The Wall Street Journal*, April 7, 2014, 1.

[29] Ibid., 10.

[30] Paul W. Parfomak. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations.* Congressional Report, Washington DC: Congressional Research Service, 2014, 4.

[31] Ibid., 4.

[32] Ibid., 4.

[33] U.S. Congress, Office of Technology Assessment. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage.* Report to Congress, Washington DC: Government Printing Office, 1990, 1.

[34] Rebecca Smith. "U.S. Risks National Blackout from Small-Scale Attack." *The Wall Street Journal*, March 12, 2014: 1.

[35] Ibid., 1.

[36] North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* Report, Washington DC: Department of Energy, 2009, 26.

[37] Headquarters, Department of the Army. *ATP 3-39.33: Civil Disturbances.* Washington DC: HQDA, 2014, 2-1.

[38] U.S. Congress, Office of Technology Assessment. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage.* Report to Congress, Washington DC: Government Printing Office, 1990.

[39] Tami Davis Biddle, “The Airplane and Warfare: Theory and History” (Carlisle, PA: U.S. Army War College, October 2013). [Blackboard], 11.

[40] Office of the Secretary of Defense. *Quadrennial Defense Review 2014*. Washington DC: Department of Defense, 2014, 7.

[41] J. Boone Bartholomes. *The U.S. Army War College Guide to National Security Issues*. 1 vols. Carlisle: U.S. Army War College, 2010, 143.

[42] Joseph S. Nye, Jr., *The Future of Power*. (New York: Public Affairs, 2011), 52.

[43] Ibid., 191.

[44] Ibid., 4.

[45] Ibid.

[46] Ibid., XV.

[47] Committee on Energy & Commerce. *H.R. 4298, the "Grid Reliability and Infrastructure Defense (GRID) Act".* March 26, 2014. http://democrats.energycommerce.house.gov/index.php?q=bill/hr-4298-the-grid-reliability-and-infrastructure-defense-grid-act (accessed March 26, 2015).

[48] Federal Aviation Administration. *FAA's major roles and responsibilities.* n.d. https://www.faa.gov/about/safety_efficiency/ (accessed March 26, 2015).

[49] Travis Holium, *Why Solar Panels Are Going on the Country's Biggest Rooftops.* December 10, 2014. http://www.fool.com/investing/general/2014/12/10/why-solar-panels-are-going-on-the-biggest-roofs-in.aspx (accessed March 7, 2015).

[50] Jo Winterbottom, *Off-grid Power Shines in India Solar Village.* August 1, 2012. http://www.reuters.com/article/2012/08/01/us-india-solar-idUSBRE8701PT20120801 (accessed March 18, 2015).

[51] Jeremy Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism.* (New York: St. Martin's, 2014), 292.