

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) 12-04-2013		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) 23-07-2012 to 14-06-2013	
4. TITLE AND SUBTITLE RISK ON THE HORIZON, RIG FOR DARK: Solutions to Mitigate DoD's Reliance on the Fragile Electric Grid				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) David L. Sagunsky LCDR U.S. Navy				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Forces Staff College - NDU Joint Advanced Warfighting School 7800 Hampton Boulevard Norfolk, VA 23511-1702				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited.					
13. SUPPLEMENTARY NOTES Information as of 29 January 2013.					
14. ABSTRACT This paper proposes that the U.S. Department of Defense faces an unnecessary risk to its capability to execute operational and strategic functions by relying on the civil electric grid. Through a basic analysis and understanding of the threats, system, impacts, and potential solutions, this paper shows how this vulnerability may be mitigated. Finally, proposed are relevant solutions in the form of on-site power generation capabilities that exist today, or are in the final design/development phases.					
15. SUBJECT TERMS Electric grid					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UNCLASSIFIED UNLIMITED	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Director, JAWS
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code) 757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL



RISK ON THE HORIZON, RIG FOR DARK:

Solutions to Mitigate DoD's Reliance on the Fragile Electric Grid

by

David L. Sagunsky

LCDR, USN

RISK ON THE HORIZON, RIG FOR DARK:

Solutions to Mitigate DoD's Reliance on the Fragile Electric Grid

by

David L. Sagunsky

LCDR, USN

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: 

12 April 2013

Thesis Adviser:

Signature: 

Prof. Frederick Kienle

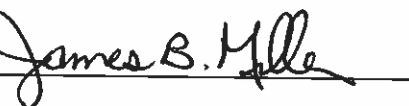
Approved by:

Signature: 

COL Richard Wiersema, USA

Signature: 

Dr. Vardell Nesmith

Signature: 

**James B. Miller, Colonel, USMC
Director, Joint Advanced Warfighting School**

ABSTRACT

This paper proposes that the U.S. Department of Defense faces an unnecessary risk to its capability to execute operational and strategic functions by relying on the civil electric grid. Through a basic analysis and understanding of the threats, system, impacts, and potential solutions, this paper shows how this vulnerability may be mitigated. Finally, proposed are relevant solutions in the form of on-site power generation capabilities that exist today, or are in the final design/development phases.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	1
Department of Defense Energy Dependence	1
The Power Grid	2
Potential Threats.....	3
CHAPTER 2: THE ELECTRICAL INFRASTRUCTURE.....	6
General Status of the U.S. Electric Grid	6
Electric Supply.....	6
Electric Transmission	8
Electric Distribution.....	9
CHAPTER 3: VECTORS FOR DISRUPTION	12
General Types of Disruption	12
Malicious Disruptions.....	12
Physical Attacks	12
Cyber-Attacks	16
Electromagnetic Pulse (EMP) Attacks.....	21
Environmental Disruptions	23
Solar Storms	23
Terrestrial Weather.....	28
CHAPTER 4: HISTORIC MAJOR BLACKOUTS OR ELECTRICAL FAILURE EVENTS	31
1859 Carrington white light flare.....	31
1989 Solar Storm	33
2003 New England Blackout	36
CHAPTER 5: POSSIBLE SOURCES OF DISTRIBUTED POWER GENERATION...39	
Threats, Risks, and Realities Need Solutions.....	39
Renewable Energy Sources	40
Solar	40
Wind.....	46
Non-renewable Energy Sources	51
Hydrogen Fuel Cells	51
Small Modular Reactors (SMR)	55
CHAPTER 6: CONCLUSIONS	62
CHAPTER 7: RECOMMENDATIONS.....	68

BIBLIOGRAPHY.....71

CHAPTER 1: INTRODUCTION

Department of Defense Energy Dependence

The Department of Defense (DoD) relies heavily on civil electrical infrastructure to provide the necessary electrical power to operate our installations.¹ The DoD's capability to exercise command and control at both the strategic and operational levels over deployed and deployable forces resides in the commands and buildings located on these installations. Communications, information technology, and their cooling systems that enable commands to carry out their functions depend on electricity. Without electricity production from some source, commands across the Department of Defense cannot accomplish their critical missions – electricity is their lifeblood.

The DoD's primary task is defending the nation in case of attack, deterring our enemies, and supporting our allies and friends. In order to accomplish this, the DoD developed complex and high tech systems of communications, weapons, and supporting functions. Many, if not most of these, rely on uninterrupted power in order to control, plan, communicate, target, and execute missions. The DoD's reliance on civil infrastructure to provide 99 percent of this electrical power leaves a major vulnerability exposed, especially in the ability of higher headquarters elements to provide and maintain strategic and operational control when civil electrical infrastructure is interrupted for more than a few hours². The thesis of this paper is that DoD should mitigate this vulnerability by developing and acquiring the capability to supply at least 30 percent of

¹ Defense Science Board Task Force on DoD Energy Strategy, "More Fight – Less Fuel", (Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, Washington, DC, February 2008), 63.

² Ibid.

installation power for a minimum of three weeks without the use of off-installation resources.

The Power Grid

The deregulation of most U.S. power grid systems has resulted in operations based on maximum-efficiency models leading in grid systems operating near maximum capacity. While this helped to maximize profits for energy companies and minimized costs to consumers, it also placed the overall U.S. power grid in a very tenuous position. Any disruption in the production, transmission, or distribution of power can or will have far reaching and cascading effects across large geographic areas. These effects will certainly include, but are not limited to, rolling or long-term blackouts, communications outages, sanitation issues as waste treatment plants go without power, clean water shortages due to water-treatment plant requirements and pumps losing power to move essential water supplies. Food will begin to spoil as refrigerators and freezers lose power, transportation will come to a halt when fuel stations cannot pump fuel, and a myriad of problems created when emergency services such as police, fire, and ambulances are saturated or communication breakdowns prevent dispatch. The longer these conditions persist, the more the problems will compound and the greater the impact on normalcy.

While most major power losses, or blackouts, only last between a few hours to at most a few days,³ there are legitimate scenarios where cascading failures will cause equipment damages requiring weeks, months, or even years to return to pre-incident operation. The cause of these incidents may be through physical or cyber-attacks,

³ Dr. Sten Odenwald, "NASA – The Day the Sun Brought Darkness," *National Aeronautics and Space Administration*, March 13, 2009, accessed August 12, 2012, http://www.nasa.gov/topics/earth/features/sun_darkness_prt.htm; "More Fight – Less Fuel", 19.

deliberate electromagnetic pulse (EMP) attacks, solar storm activity, or even terrestrial weather. Any one of these could lead to the kind of cascading failures that can cause catastrophic electrical infrastructure equipment damage requiring weeks to years to repair or replace. DoD systems would be impacted the loss of network systems, communications, and electricity to run the computer systems necessary for planning and directing dispersed DoD units.

Potential Threats

This array of threats is not just in the fevered imagination of pessimistic conspiracy theorists. General Keith B. Alexander, USA, the Director of the National Security Agency and Commander, U.S. Cyber Command, revealed that there was a 17-fold increase from 2009 to 2011 in computer attacks on U.S. infrastructure to include the electric grid, transportation, and oil supply systems.⁴ Cyber-attacks have been a threat for some time, but now reports exist throughout the world as individual hackers as well as governments use the cyber domain to attack and cause damage to computer systems controlling various networks. Cyber-attack is increasingly becoming a threat to energy production and distribution systems.

The threat of Electromagnetic Pulse (EMP) attacks has also garnered substantial research for over 50 years. In 1962, the United States conducted high altitude (400 km or 250 miles) nuclear detonation tests. Unexpectedly, electrical systems 1,400 km (875 miles) away suffered interference, disruption, and damage because of the EMP created by

⁴ David E. Sanger and Eric Schmitt, "Rise is Seen in Cyberattacks Targeting U.S. Infrastructure", *The New York Times*, July 26, 2012, accessed December 17, 2012, <http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?ref=stuxnet&r=0>.

the nuclear detonation.⁵ Also in 1962, Soviet nuclear testing reported observing damage to overhead and underground cables, surge arrestor burnouts, spark-gap breakdown, blown fuses, and power supply breakdowns up to 600 km (375 miles) away.⁶ This helped to confirm the impact of EMP effects and the fact that merely burying electric cables would not prevent the powerful electrical pulse from travelling along those cables to locations where they could cause equipment damage.

Solar and terrestrial storms pose yet another real threat to the electric grid. Normal storms and their associated winds can cause widespread blackouts from trees and associated debris by damaging power lines. This occurs all over the world every year, in every season. Documented solar storm activity is capable of overloading critical infrastructure nodes and causing permanent and catastrophic damage to equipment.⁷ Because preventing these naturally occurring events is not possible, the only realistic option is to mitigate the effects through equipment design and distribution to prevent network nodes that become single points of failure.

Along with these risks, the continued high demand on the electric grid is at a level where little extra capacity exists to shift from one region to another. This is partly due to the effect of companies trying to maximize profit margins without increasing prices and therefore not investing in expanded capacity. In addition, partly because the industrial infrastructure components of an electric grid, such as transmission lines, transformer substations, and power plants, are not particularly aesthetically pleasing, there is a

⁵ William Graham on July 21, 2009, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong., 1st sess.

⁶ Ibid.

⁷ John Kappenman prepared testimony on April 30, 2012, before the U.S. Federal Energy Regulatory Commission at the *Technical Conference on Geomagnetic Disturbances on the Bulk Power System*, docket #AD12-13-000. A transformer at the Salem New Jersey nuclear power plant was destroyed as a result of geomagnetic induced currents created by the solar storm observed in March 1989.

general feeling among individuals that they do not want to have these infrastructure components near their residential or non-commercial properties. Therefore, DoD is left in a precarious position where it is reliant on electricity but has very little influence on electric companies to invest in making the grid more resilient and therefore more secure. The solution that remains is for DoD to take the steps, and investments if necessary, to enable on-site, long-duration electricity generation without relying on an off-site supply of fuel.

With all of the outlined threats to the stability of the U.S. electric grid and its overall fragility, DoD cannot turn a blind eye and hope that someone else will take the actions necessary to ensure a stable and secure network of electrical power. DoD should develop and acquire the capability to supply at least 30 percent of installation power for a minimum of three weeks without the use of off-installation resources. In the following chapters, this paper explores the major components of the U.S. electric grid and threat vectors that exist and may be exploited causing system failures. In addition, illustrative major electric grid failures or electric power events in the past are reviewed as well as the current state of possible alternative solutions for DoD installations to produce a portion of their own power without relying on the rest of the electric grid. Finally, this paper postulates initial workable conclusions regarding the vulnerability DoD faces in reliably carrying out its critical primary functions and make recommendations on how to reduce or possibly eliminate some of these vulnerabilities.

CHAPTER 2: THE ELECTRICAL INFRASTRUCTURE

General Status of the U.S. Electric Grid

Electric Supply

To understand fully the vulnerability that the Department of Defense (DoD) incurs from its reliance on the civil electric grid, it is necessary to understand the components that comprise the main electric grid elements. This helps identify the critical nodes and begins to shape the understanding of each component's vulnerabilities to disruption, through either natural occurrences or deliberate malicious intent. The potential vectors of disruption are discussed in Chapter Three along with how each portion of the U.S. electric grid is more or less susceptible to each disruptive influence.

The U.S. electric grid infrastructure consists of interconnected regional webs of supply, transmission, and distribution equipment of varying capacity (voltage), complexity, and age. Each component of these regional webs has its own unique characteristics that influence the level of performance, resilience or vulnerability. These characteristics also vary from one region to another based on the threat. Different malicious threats can target or disrupt different characteristics based on the desired effects and capabilities of the attacker. Other natural threats and their effects vary by geographical region in ways that will be further discussed in Chapter Three.

The U.S. electric supply consists primarily of more than 6,000 large power generation facilities,¹ generating through several production methods, distributed throughout the country. For comparison, there were nearly 3,800 Wal-Mart stores in the

¹ James A. Marusek, "Solar Storm Threat Analysis," *Impact*, published 2007, accessed September 4, 2012, <http://www.breadandbutter-science.com/SSTA.pdf>.

United States in 2005.² This illustrates the prolific number of utility-scale power generation facilities spread across the United States. The method of electric production varies and includes coal, natural gas, oil, nuclear, hydroelectric, wind, solar, and biomass. Additionally, the number of generation facilities of each method does not necessarily correlate with the amount of overall power produced. For example, nuclear power facilities only make up 0.6 percent of all power generation facilities in the U.S., but they account for 9.4 percent of the electricity produced.³ Natural gas and coal remain the top two sources of electric power in the U.S. accounting for just over 70 percent of the 2010 electricity production in the U.S.⁴ Most electric power generation facilities for all methods are comprised of large buildings with personnel physically on site to carry out the daily operations and maintenance required. Wind farms and solar arrays, however, are concentrated over an area but not contained within a building. Except for periodic on-site maintenance, remote facilities conduct the daily monitoring and control. This physical presence, or lack thereof, and its impact of facility security will be further addressed in Chapter Three.

While the power produced at these major power facilities is necessarily large in order to meet the electric demand, they do not have much spare capacity. For example,

² Matthew Zook, Mark Graham, "Wal-Mart Nation: Mapping the Reach of a Retail Colossus," in *Wal-Mart World: The World's Biggest Corporation in the Global Economy*, ed. Stanley D. Brunn (New York: Taylor & Francis Group, 2006), 16.

³ US Energy Information Administration, "Electric Power Annual 2010 Data Tables, Table 1.2 Existing Capacity by Energy Source, 2010 (Megawatts)," accessed December 14, 2012, <http://www.eia.gov/electricity/annual/html/table1.2.cfm>. Electricity generation facilities by percent of utility production: natural gas - 31, hydroelectric - 22.1, oil - 20.8, biomass - 8.7, coal - 7.7, wind - 3.8, solar - 1, nuclear - 0.6, other - 0.3. Utility electricity production by percent: natural gas - 41.3, coal - 30, nuclear - 9.4, hydroelectric - 6.9, oil - 5.5, wind - 3.5, biomass - 0.4, solar - 0.1, other - 0.1.

⁴ Ibid.

U.S. nuclear plants were operating at 90 percent of generation capacity in 2011.⁵ Federal regulations only require each power plant to have a reserve capacity of approximately 10-15 percent of peak demand.⁶ Since each power facility has a certain design capacity relative to the geographic area it supplies, any increase in the normal demand within that area pushes normal demand closer to the peak, rather than normally expected, demand anticipated when the facility was designed and built. As areas grow in population and our appetite for electric power grows, this puts an ever-increasing demand on existing power generation systems.

Without the introduction of new power production facilities of any or all methods, the electric power grid will only become more fragile as greater demands are placed on a static supply capacity. As the demand increasingly reduces the spare capacity, any interruption of the production or transmission of electricity will result in the inability of another grid geographic area to help meet the extra demand. Operating with such minimal spare generation capacity or resiliency leaves DoD installations vulnerable to increasingly frequent, and longer duration, electric power outages.

Electric Transmission

A combination of regional, and limited national, network power lines of various capacity facilitate the transmission of electricity produced by electric power generation facilities. The high-power transmission lines currently carry four voltages (230 kilovolts (kV), 345 kV, 500 kV, and 765kV) depending on the particular system.⁷ (For comparison, the standard end-user voltage in the United States is 110 volts with some

⁵ Marcus King, LaVar Huntzinger, and Thoi Nguyen, "Feasibility of Nuclear Power on U.S. Military Installations" (CNA report commissioned by the U.S. Department of the Navy, March 2011), 18.

⁶ Micahel Barrett, "Ensuring the Resilience of the U.S. Electrical Grid; Part III: Requirements for a More Resilient System" (Lexington Institute, Arlington, VA, November 2012), 2.

⁷ Marusek.

appliances, such as clothes driers, using 220 volts.) The high-voltages on these lines allow for transmission of electricity over long distances with a minimum of power loss. These high-voltage lines then connect to smaller lines carrying lower voltages to neighborhood substations and large businesses such as factories that use voltages greater than 110 or 220 volts. Finally, the voltage is stepped down one final time before entering the electrical system of the building, facility, or home of the end user where it powers such things as lighting, heating and air conditioning units, and providing power to computers and other electronic devices. Step-down transformers facilitate this process of taking high-voltage power and converting it to a lower voltage useable by a consumer. The transmission network is both complex and extensive.

In order for the entire electric transmission system to work, stepping up voltages from the generation facilities for transmission is required and then stepped back down for end users. This requires a complex network of infrastructure, costly equipment, maintenance, and steady operations. Any interruptions in this network due to damage, malfunction, or even necessary periodic maintenance can result in end users being without electric power until the equipment causing the interruption is repaired, replaced, or otherwise returned to operation. The amount of time for this to occur will vary greatly based on the type of interruption, its geographic location, and whether another part of the grid has enough excess capacity to share the electrical load.

Electric Distribution

The distribution network consists of transformers connected to the transmission lines and either increases the voltage for long-distance transmission or decreases it for transmission on lower-voltage systems or for end user consumption. These transformers

vary in size from the relatively small cylinders seen on power poles outside of homes to some that weigh almost 100 tons and can be as large as a small house in physical dimensions.⁸ While the small transformers are generally standard in size, shape, and design, the large, high-voltage ones connected to the long-distance transmission lines are each custom built and designed for their particularly specified requirements. These transformers take an average of one year to design and build, cost upwards of millions of dollars, and only one company in the world (located in Canada) manufactures 765 kV transformers.⁹ Additionally, the large transformers are located in transformer stations that are generally unguarded, unsecured, and exposed with little more than a chain link or similar fence to prevent anyone or anything from wandering in among the station components.

These various transformer stations, integral to the power transmission and distribution, are critical nodes in the electric power grid. If they become damaged, destroyed, or removed from service for any other reason, the load placed on the remaining transformers increases. Each node affects the other. As these critical components begin operating closer and closer to their maximum capacity, their life spans shorten similar to any other piece of equipment operating at or near its 100 percent capacity.

It is difficult to estimate how much of the overall grid is operating at a specific percent of its capacity because each generation facility feeds into different demands and different areas have seen broad changes in the demand. However, as an illustrative example of the increasing demand placed on the U.S. electric grid, as of 2011, U.S.

⁸ Ibid, 6.

⁹ "More Fight – Less Fuel," 55.

nuclear plants were operating at 90 percent of generation capacity, as opposed to 1980 when they were operating at 56 percent capacity, according to a U.S. government study.¹⁰

The narrowing margins of capacity-to-demand coupled with the long lead times required to obtain replacement components increases the risk that widespread longer-duration electric grid failures will become more frequent. As U.S. society and DoD have become dependent on electricity to perform normal functions, the impacts resulting from interruptions are increasing. A loss of electricity greatly diminishes the U.S. government's ability to provide effectively the services required of it. Losing electric power could be catastrophic to DoD's ability to conduct operations, planning, and exercise command and control functions. The next chapter discusses potential vectors to cause a widespread, long-duration electric grid failure. Some of these could be maliciously directed for an adversary's benefit, and others could simply provide an opportunity for an adversary to take actions to which DoD would be unable to present a coordinated response. Regardless of the threat vector, the precipitously balanced and dispersed, interdependent electric network is essential to DoD's mission capability.

¹⁰ King, Huntzinger, and Nguyen, 18.

CHAPTER 3: VECTORS FOR DISRUPTION

“Our military installations are vulnerable because they rely on an insecure electric grid.” - Congressman Bennie G. Thompson (D-MS) ¹

General Types of Disruption

Malicious Disruptions

Physical Attacks

Physical attack of the electric grid infrastructure is the simplest to describe and visualize for every component of the grid. It could take the form of attacks by adversary nations, groups, or even individuals. Some examples of physical attacks could be explosives on supply facilities, transmission lines, or transformer stations, cutting trees to fall across power lines, or multiple other acts limited only by the imagination and determination of the attacker. In fact, physical attacks on the electric grid in Iraq and Afghanistan have been (and continue to be in Afghanistan) “one of the most common and effective tactics” used by insurgents.² With very little effort using an internet connection, a small group could identify the locations multiple targets and may be able to conduct a coordinated attack with a high probability of success and low risk of capture due to the chaos created by electric power failures.

As shown in recent conflicts, it has become more common to disrupt power generation for political, military, or ideological purposes or to accomplish specific ends. Various law enforcement and intelligence agencies discovered and thwarted several plans

¹ Chairman Bennie G. Thompson (D-MS), July 21, 2009, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong., 1st sess.

² “More Fight – Less Fuel”, 63.

to attack the U.S. electric grid physically.³ The U.S. military also intentionally and successfully targeted other countries' power grids in the execution of operations.⁴ In the 1991 Persian Gulf War, the U.S. led coalition targeted and destroyed specific nodes in the Iraqi electric grid in order to incapacitate the Iraqi command and control network.⁵ This kind of planning and execution is no longer solely resident in nation-state actors but non-state actors have the ability to carry out similar operations to disrupt electric generation and distribution.

Disrupting power grids can be more than disruptive; it can be catastrophic to the Department of Defense's (DoD) ability to execute its primary mission of defending the United States and its citizens. While the 1991 action did accomplish its primary mission of disrupting, and in some cases eliminating, the Iraqi air defense systems and ability to coordinate the actions of its other forces, there were major unintended consequences. One consequence was that key power nodes also supplied power to civil water purification plants. Without clean water, a health crisis fomented that severely strained the Iraqi hospitals and health systems.⁶ If the U.S. used this kind of attack to facilitate the achievement of military objectives, it is very likely that others who would wish the U.S. harm could use similar methods. It is conceivable that criminals, terrorists, or other enemies of the United States might want to attack critical infrastructure nodes to attain their own ends or meet their own intentions to cripple various U.S. capabilities or the U.S. lifestyle.

³ David E. Sanger and Eric Schmitt, "Rise is Seen in Cyberattacks Targeting U.S. Infrastructure", *The New York Times*, July 26, 2012, accessed December 17, 2012, <http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?ref=stuxnet&r=0>.

⁴ Elaine M. Grossman, "Effects-based Operations Under Fire: A Top Commander Acts to Defuse Military Angst on Combat Approach," *Inside the Pentagon*, April 20, 2006.

⁵ Ibid.

⁶ Ibid.

The most critical infrastructure nodes in the electric grid are the large transformers.⁷ These components act as the connective tissue in the entire system. They are located at both power generation facilities to step-up the voltage for transmission and to step-down the voltage for local distribution and use. Many of these step-down transformers are in places easily accessed by roads and are generally found near population centers. As previously noted these large step-down transformers do not require on-site monitoring and frequently protected only by a chain link fence that leaves them at risk. The power companies that own and operate the equipment consider this level of risk fiscally acceptable. A business model is the basis for their risk calculations. DoD installations cannot accept the same level of risk to the uninterrupted supply of electricity.

In addition to the paucity of security surrounding these large transformers, there is a very limited capacity to build new ones. As noted, only one company in the world produces transformers for 765 kV systems, and it is located in Canada.⁸ Due to the unique specifications for each and the complexity involved in their production, these transformers take an average of one year to build.⁹ With the destruction of several of these transformers, large sections of the electric grid could remain without power for months, or even years, while building replacement transformers or generation facilities within the local distribution area that would not require the electricity to travel over the

⁷ Dr. William Radasky, with Mr. John Kappenman, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong., 1st sess., July 21, 2009. While Dr. Radasky and Mr. Kappenman's prepared statement was focused on the vulnerabilities to electromagnetic pulses and geomagnetic storms, the conclusion of component risk holds true for physical attacks as well.

⁸ "More Fight – Less Fuel," 55.

⁹ Graham, William.

high-voltage transmission lines.¹⁰ Even without doing a formal risk analysis process or possessing a background in electrical engineering, it is reasonable to conclude that these transformers may be the Achilles heel of the U.S. electric grid.

Power lines are also a component of the electric grid that is highly vulnerable to physical attack. Destroying or rendering power lines inoperative is a simple task achieved through a number of possible methods to include cutting, explosion, felling of support poles or towers, and other destructive options. High-voltage power transmission lines often span long distances, sometimes through extremely low population density areas. This presents an attacker with a higher probability of successfully committing a malicious act and then vacating the area before anyone could respond to catch the perpetrator. These remote and sometimes barely accessible locations also require more time for repair crews to reach the damaged lines. Once again, this does not have to be a highly complex attack nor would it require a great deal of effort to carry out. High-voltage transmission lines present a lucrative target that can have an immediate impact on power generation and transmission services.

One disadvantage to anyone attacking power lines, however, is that repair and power restoration is relatively easy. Unlike high-voltage transformers, the components are not unique so there is a much more ready supply of replacement parts. Additionally, the support structures holding these power lines consist generally of wooden poles or metal frames that have short fabrication and replacement or repair timelines. Because they are ubiquitous, power transmission lines present a ready target for temporarily disrupting an electric power grid. However, because they are so common, they would not provide the long-term effects that emerge from a successful attack on transformers or

¹⁰ Radasky and Kappenman.

even generation facilities. The fact that these support structures are easy for an attacker to reach also means that repair crews can also reach them easily which helps to mitigate any disruption.

Probably the most complex part of the electric grid infrastructure to attack is the power generation facilities. For most of these facilities, people work on site for daily operations, maintenance and security. However, this paper does not delve deeply into the strengths and weaknesses of each kind of facility due to the tremendous variation in susceptibility based on location, physical construction, security measures, and robustness of the generating system. While the consequences of a successful attack could be disastrous due to the long duration of power loss and long time required to repair or replace the facility, those who may look to interfere with the U.S. electric grid will most likely seek the highest reward with the lowest risk of mission failure or capture. Short of a spectacular 9-11 type attack, it can be generally stated that the power generation facilities would be the most difficult to attack physically and thus the least likely to be targeted for such an attack.

Cyber-Attacks

Recently, the public has become much more aware of the reality and likely capability of a cyber-attack. National and international media has widely publicized the Stuxnet virus found in Iran's nuclear program computer systems that caused centrifuges to either shut down or act in ways that led to physical damage. In fact, physical damage occurred to approximately 1,000 centrifuges at Iran's Natanz nuclear facility and required replacement. Video imagery obtained by International Atomic Energy Agency inspectors clearly showed this physical wreckage and clear evidence of the removal of equipment

that had been working normally prior to the Stuxnet attack.¹¹ A demonstration of the potential for a damaging cyber-attack has occurred in Iran beyond any reasonable doubt.

The damage caused by Stuxnet resulted from commanding the centrifuges into over- and under-speed conditions. This led to thermal deformation of the aluminum centrifuge tubes, which then contacted adjacent structures resulting in mechanical failure.¹² Other, less well-reported incidents have occurred as well. The U.S. Congress has held more than 75 hearings since 2005 in order to understand fully the vulnerability of our society to a cyber-attack and what can be done to prevent, or limit the impact of, a successful cyber-attack.¹³ This area demands immediate research and understanding in order to prevent or mitigate a successful cyber-attack on U.S. electrical production. The proven cyber-attack vector is a serious threat further complicated by the increased reliance on computer-based systems monitoring and controlling power generation.

This attack vector could be one of the more difficult problems to solve as most power companies have moved to a system of central monitoring and control stations that can operate large sections of grids remotely via computer systems connected through the internet.¹⁴ As each company develops its own unique programs and systems, each retains a different level of security, vulnerability, and redundancy. Because of this, no single program or set of preventative measures will be able to achieve a reasonable level of

¹¹ Norman Asa, via PR Newswire, "Cyberattacks on Iran – Stuxnet and Flame," *The New York Times*, August 9, 2012, accessed December 17, 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

¹² Holger Stark, "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War", *Spiegel Online International*, August 8, 2011, accessed December 17, 2012, <http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-or-cyber-war-a-778912.html>.

¹³ CQ Transcripts, *CQ.com*, accessed February 20, 2013, <http://cq.com/transcripts/newsmaker.0>. Results based on a search of Congressional hearings specifically related to "cyber" issues.

¹⁴ Paul H. Gilbert, PE, on September 4, 2003, before the Committee on House Homeland Security Subcommittee on Infrastructure and Border Security, 108th Cong., 1st sess.

protection across all of these disparate systems. A 2005 Presidential committee found that “computers that manage critical U.S. facilities, infrastructures, and essential services can be targeted to set off system-wide failures, and these computers frequently are accessible from virtually anywhere in the world via the Internet.”¹⁵ With the great variation in control systems in terms of age, supplier, user designed programs, and user protocols, there will be no simple solution to the threat of cyber-attacks. Even if an electric company were to expend the resources to construct a network for its distributed control systems that was completely independent of the internet, the elimination of threatening malicious code introduction is still not possible.

In addition, foreign countries such as China and India write a large amount of critical electric infrastructure control and management software.¹⁶ This opens the possibility for malicious code being introduced into the software at the component’s production source making the harmful code extremely difficult, if not impossible, to identify before installation. Electric companies have accepted this risk based on the cost and availability of acquiring components domestically and, it can be assumed, determined that the greater expense of domestically produced components was not justified based on their assessment of the likelihood of tampering. Again, DoD cannot use the same business-model risk analysis when the consequences are more than just a loss of revenue or customer dissatisfaction.

Cyber-attacks through the internet and through malicious code implanted during component manufacturing are serious threats. The Defense Science Board Task Force on

¹⁵ President’s Information Technology Advisory Committee, report to the President, “Cyber Security: A Crisis of Prioritization”, February 2005, 5.

¹⁶ Thomas X. Hammes, COL, USMC, *The Sling and the Stone: On War in the 21st Century*. (Minneapolis, MN: Zenith Press, 2004) 260.

DoD Energy Strategy conducted a detailed analysis of the potential for and consequences of cyber-attacks. Due to the possibility of exploitation by hostile entities, this analysis is as a classified annex to their report “More Fight – Less Fuel.”¹⁷ In deference to the seriousness recognized by the Defense Science Board Task Force, a summary of this classified annex will not be included but is available to those with proper credentials. The report does confirm, however, that cyber-attacks are a substantial risk with serious consequences.

Of the three main components of the electric grid, power generation facilities would be the most vulnerable to cyber-attacks due to their control systems. The vector of attack could be either through an insider threat or via an off-site attack through the internet. In 2007, the Department of Homeland Security in conjunction with the Department of Energy’s Idaho National Laboratory, conducted an experiment called “Aurora.” The purpose of the experiment was to see if it was possible to cause physical damage or destruction of a large generator via a cyber-attack. The experiment was successful in destroying the generator used in the test beyond the capability of repair.¹⁸ Like the Stuxnet virus, the “Aurora” experiment clearly and definitively demonstrated that a cyber-attack could cause a system to operate in a manner that ultimately causes its own destruction. The level of sophistication needed to accomplish this will vary, among other factors, depending on the equipment targeted, infection method, and the degree of anonymity the creators wish to maintain.

¹⁷ “More Fight – Less Fuel”, 55-56.

¹⁸ Congressman James R. Langevin (D-RI), October 17, 2007, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 110th Cong. 1st sess.

An “insider threat” from a cleared and trusted employee could be the most dangerous due to legitimate familiarity with the systems and their normal operating parameters and vulnerabilities. The “insider threat” may come from an employee carrying out an attack through manipulation or coercion, or it could be a disgruntled employee. Either way, the resident knowledge of a control system’s weaknesses means that this is another vector within the cyber realm that DoD must consider in the reliability of the electric grid upon which it depends. In contrast, a sophisticated external threat could also wreak considerable damage while remaining safe and unaffected due to the ability to conduct the attack from a location anywhere in the world using a connection to the internet. This anonymity also makes it extremely difficult to track the attackers back to their source.

With a sophisticated off-site attack, it is possible for a hostile actor to affect the United States’ ability to respond or continue operations already underway. The kind of responses, and legal authorities available for responses, are beyond the scope of this paper, but it remains important to have measures in place to define how we can respond to a cyber-attack. One of the significant requirements for this response is to identify positively the party responsible for conducting the attack. If a cyber-attacker can remain completely anonymous, then no level of deterrence will ever be effective and there is no downside consequence for the attacker.

The threat of a cyber-attack is real. Stuxnet and “Aurora” demonstrate that they can be effective. The electric industry’s ability to protect itself from these attacks will remain limited due to their fiscal constraints and multitude of different operating systems

and components. DoD must take action to reduce its reliance on this fragile and cyber-attack vulnerable network.

Electromagnetic Pulse (EMP) Attacks

An electromagnetic pulse (EMP) can also damage or destroy parts of the electric grid through sudden and powerful electric surges. One method of creating an EMP is through a high altitude nuclear detonation. These detonations, at altitudes between 40 - 400 km (25-250 miles), are high enough that no blast effects are felt on the ground.¹⁹ However, the high-energy radiation released does propagate to the Earth's surface in the form of an electromagnetic pulse.²⁰ The resulting EMP affects everything within range, limited only by the line of sight from the detonation.²¹ EMP is an ever-present threat to all electrical equipment and science and government experts recognize this.

Mr. William Graham, the Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse, emphasizes that the impact of an EMP on the United States and other modern infrastructure societies could be devastating. He notes with regard to EMP, "It has the capability to produce significant damage to critical infrastructure and thus to the very fabric of U.S. society, as well as the ability of the U.S. and Western nations to project influence and military power."²²

As illustrated in Figure 1 on the following page, two high altitude nuclear detonations could create EMP effects covering nearly the entire continental United States. This would cause simultaneous electrical system failures, and even systems that have been hardened for protection against EMP may still be susceptible to the power surges

¹⁹ Graham, William.

²⁰ Radasky and Kappenman.

²¹ Graham, William.

²² Ibid.

created in the electric grid. Imagining the consequences of a simultaneous failure of electronic equipment is not pleasant, but neither is it difficult. Computer systems simultaneously shutting down, all lights going out, pumps maintaining pressure in natural gas lines cease operating, and car engines shutting off due to the electronic control systems failing are just a few of the consequences of an EMP attack. An adversary with a nuclear weapon capable of delivery by even a short-range ballistic missile could achieve all of this.

The accuracy of an EMP attack would not need to be very good in order to achieve the attacker's desired effects, within a few tens of miles would be sufficient. In addition, the level of technical skill required to produce a viable reentry vehicle would not be necessary, as an EMP detonation would most likely occur exo-atmospherically to achieve the largest area of effect.

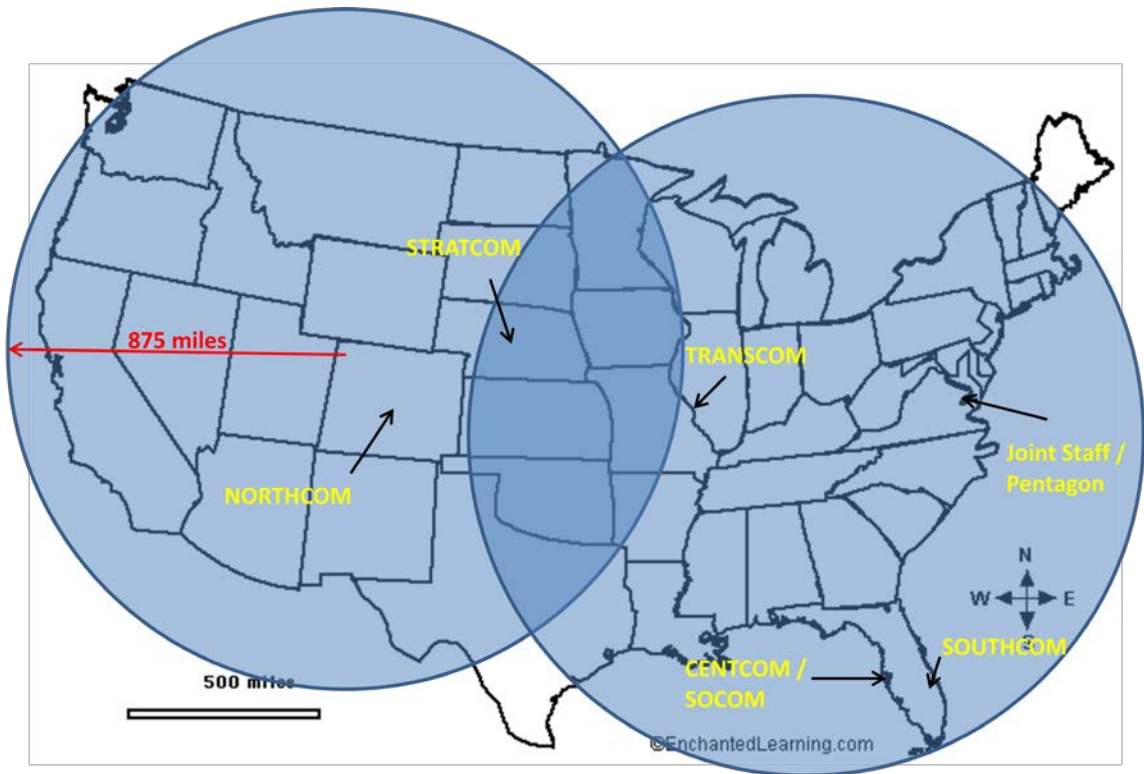


Figure 1 – Graphical depiction of two 875 mile radius circles representing the EMP effects range of an EMP scenario similar to those observed in 1962 nuclear detonation tests.²³ This illustrates that only two EMP detonations would affect nearly the entire continental United States.

Environmental Disruptions

Solar Storms

One significant type of naturally occurring event that could disrupt the production and delivery of power is a solar storm. Solar storms can create effects in the earth's magnetic fields resulting in geomagnetic storms. EMP and geomagnetic storms share a strong relationship in how they can affect the electric grid and infrastructure. While the generation methods are very dissimilar, the electric and magnetic waveforms and their impacts are very similar.²⁴

²³ Graham, William.

²⁴ Radasky and Kappenman.

The following discussion of solar storms is in two parts to understand better the threat vector and to understand how they can affect the electric grid. First is a short overview of solar storms themselves, their frequency, and their measurement. Following that is a description of solar storm effects when they hit the Earth. While many do not often consider solar storms, their potential for disruption is evident.

The magnetic fields within the sun undergo a 22-year cycle during which the magnetic poles reverse every 11 years.²⁵ While the poles reverse, increased solar storm activity results in the sporadic release of intense electromagnetic energy. Measurements of the magnitude of these storms fall into three classes, C, M, and X based on the intensity of a particular wavelength of x-rays emitted. X class storms are the most powerful. Within each class, the intensity is further broken down from 1 – 10 for classification that is more specific. This scale is linear, so an X2 storm is twice as powerful as an X1, and an X5 is five times more powerful.²⁶ As an exception, X class storms can go beyond an X10 rating with the number directly correlated to the intensity of x-ray energy released by the storm. As a rule, X class storms are the only ones with enough energy to cause any more terrestrial effects than some minor communications interference and an increase in the aurora borealis. Therefore, this paper will only focus on the disruptive capabilities of X class storms.

The major component of a solar storm that affects the Earth is the Coronal Mass Ejection (CME). A CME is a massive ejection of plasma from the sun caused by sudden magnetic stress seen as sunspots.²⁷ Contained in this CME are low- to medium-charged

²⁵ “The Sun’s Magnetic Field,” NASA’s Cosmicopia, last modified May 11, 2012, accessed December 19, 2012, <http://helios.gsfc.nasa.gov/solarmag.html>.

²⁶ Marusek.

²⁷ Odenwald.

particles and a powerful, compact magnetic field.²⁸ The more powerful the storm that created the CME, the more energetic it is and the faster it travels. In some observed geomagnetic storms, the CME reached the Earth within only a few minutes of its release from the surface of the sun.²⁹ The CME's impact can be near instantaneous and is nearly impossible to anticipate. While there is some ability to predict periods when a solar storm is more likely, models do not currently exist to predict their severity and timing.

As stated earlier, solar storm activity follows the normal solar cycles of polarity reversal. Typically, these peak periods will produce two to three large storms.³⁰ Following this cyclic pattern, historical evidence shows that a storm with the potential for major impact to the electric grid occurs approximately every 30 years.³¹ Table 1 below shows a historical record from 1859 to 2003 of major solar storms. With slight variation, major storms occurred on a relatively regular interval of approximately 11 years.

Sep 1-2, 1859 (Carrington white light flare)	May 13-16, 1921
Oct 12, 1859	Jul 7, 1928
Feb 4, 1872	Apr 16, 1938
Nov 17-18, 1882	Sep 13, 1957
Mar 30, 1894	Feb 11, 1958
Oct 31, 1903	Mar 13, 1989 (X15 class)
Sep 25, 1909	Oct 28 – Nov 5, 2003 (three major storms)

Table 1 – From October 28 to November 5, 2003, recordings of three major storms resulted in the following classifications: Oct 28 – X17.2; Oct 29 – X10; Nov 4 – X45. The November 4 storm is the largest solar storm ever directly measured. While observed, the Carrington white light flare was not measured.³²

²⁸ Marusek.

²⁹ Radasky and Kappenman.

³⁰ Odenwald.

³¹ Radasky and Kappenman.

³² Marusek.

When a CME reaches earth's magnetic field, it causes a temporary disturbance and intensification of the fields that can last from hours to days.³³ This is most visible in the form of aurora borealis sightings in much lower latitudes. As more intense fields penetrate into the ground, resistance builds up resulting in fluctuating electrical and magnetic fields.

Following Faraday's Law, power lines stretched through these fluctuating fields pick up current. These Ground Induced Currents (GIC) and their magnitude are a function of the length of the power line exposed to the fluctuations and the intensity of the fluctuating field. As a further variable, the type of rock formations in the ground affects the ground's resistance to the fluctuating magnetic field. As the resistance increases, such as happens in igneous rock formations, the power of the GIC is increased.³⁴ Locations closer to the magnetic poles are more susceptible to these fields due to the path of Earth's magnetic field lines. For example, the U.S. East Coast at mid-latitudes is more at risk from GICs than the U.S. West Coast at the same latitude due to proximity of the magnetic north pole.³⁵

Two major geographic features place the U.S. Eastern Seaboard at a high risk of disturbance. The first, as noted, is its geographic location relative to the magnetic north pole. The second is that there are large portions of the U.S. Eastern Seaboard that have underlying igneous rock formations.³⁶ With large population concentrations within this higher risk area, the ability to mitigate grid wide power outages can make the difference between temporary disruptions to long-term outages for possibly millions of citizens.

³³ Ibid.

³⁴ Odenwald.

³⁵ Ibid.

³⁶ Ibid.

The negative effects on large populations with over large geographic areas for extended periods can be devastating.

As a GIC enters high power transmission lines, it flows to the step-up and step-down high voltage transformers at either end. As this current is neither metered nor regulated, it can result in major damage or destruction to these transformers. The out-of-phase currents can cause the transformers to overheat and even to vibrate strongly enough to cause physical damage to components.³⁷ The impact of this is that damaged step-up transformers may prevent power generation facilities from transmitting their power, or the available power may not be able to be distributed from the high-voltage transmission lines because of failures in the step-down transformers.

While a major geomagnetic storm is a low-frequency event, their impacts can be severe and have the potential to persist for long periods. As recognized by Mr. Joe McClelland, the Director of the Office of Reliability, Federal Energy Regulatory Commission,

...the power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced power spikes. The collapse of numerous transformers across the country could result in reduced grid functionality or even prolonged power outages.³⁸

Mr. McClelland went on to state that,

Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens.³⁹

³⁷ Kappenman, docket #AD12-13-000, April 30, 2012.

³⁸ Director Joe McClelland, July 21, 2009, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong., 1st sess.

³⁹ Ibid.

A major solar storm hitting Earth is not a probability it is a certainty. The only questions are when will it occur? How intense will it be? How long will it take the electric grid to recover? Has DoD prepared its installations to be resilient enough to absorb the resultant loss of power from the electric grid? The answers to these questions will largely determine whether DoD installations and their essential tenants will be able to continue operations or simply have to wait helplessly for the civil grid to be restored.

Terrestrial Weather

Violent weather, such as blizzards, thunder storms, or other weather systems causing violent weather are the most common cause of power outages or blackouts. After any major storm, local media rarely fail to provide images of trees that have fallen across power lines or power poles that have been knocked over with their lines broken. This kind of damage is relatively simple to repair and generally, power restoration to nearly all customers is a matter of hours; however, larger storms such as hurricanes and Nor'easters can cause physical damage beyond just downed power lines. They nearly always do that, and in numerous locations, which increases the number of repairs required, but additionally, they can cause damage to the power generation facilities and transformer stations in the form of structural damage and flooding.

While meteorologists possess the ability to forecast much of this level of destructive weather with a reasonable level of certainty, no one yet has the capability to prevent it. Thunderstorms and tornadoes sometimes only allow a few hours, or minutes, forecast due to their rapid growth, but they are generally part of a seasonal norm in geographic areas. Being able to predict exactly where a power line may be damaged by broken limbs, fallen trees, or damaged transmission line supports caused by high winds is

impossible, but general areas where storm effects will be highest can be forecast with a reasonable degree of accuracy. This allows companies to prepare repair crews in advance respond quickly to any damages that do occur. This preparation in advance of a storm helps to allow planning and preparation to minimize the duration of any power interruption.

With globally distributed locations, DoD facilities will experience all of these weather types at one time or another. As an example at an illustrative tactical level, when recent Superstorm Sandy hit New Jersey and New York City on October 29, 2012, the New York Army National Guard 69th Infantry Regiment lost power at their armory at 25th street and Lexington Avenue in Manhattan. Without sufficient backup power, they had no lights, radios, computers, or heat. In a stroke of luck, Victoria's Secret was on-site preparing for their annual fashion show and had eight 500-kilowatt generators. By rigging these generators to the building's electrical system, the 69th Infantry Regiment was able to restore all of the lost power and electrically reliant capabilities.⁴⁰ Had these generators not been on-site and available, it is questionable how effective this National Guard unit would have been in helping to provide disaster relief. At one point, the Guardsmen had to carry physically diesel fuel up 13 stories to keep a hospital generator on-line for a patient in such critical condition that moving him was not an option. It required 30 Guardsmen working 12-hour shifts and continuously carrying fuel to keep one generator functioning.⁴¹ It is now easier to imagine the difficulty that would exist in

⁴⁰ Noah Shachtman, "How Victoria's Secret Saved the National Guard During Hurricane Sandy," *Wired.com*, posted November 2, 2012, accessed December 19, 2012, <http://www.wired.com/dangerroom/2012/11/victorias-secret-sandy/>.

⁴¹ *Ibid.*

a situation where the power is out over a much larger area with no immediate relief supplies available in appreciable amounts.

The possible threat vectors to the electric grid discussed in this chapter are merely a sample of items that have caused failures in electric systems. Each vector acts through different means, but each can be mitigated with on-site electrical power generation at DoD installations. By creating installations that are more independent of the electric grid, DoD will ensure its capability to carry out critical functions in times of crisis.

CHAPTER 4: HISTORIC MAJOR BLACKOUTS OR ELECTRICAL FAILURE EVENTS

The following examples of major blackouts or electrical events demonstrate the witnessed effects of power outages and, in the case of the 1859 solar storm, the effects on even basic electric systems from solar activity. Actual examples of the resultant situations from some of the possible threats described earlier, these historical examples illustrate some of the risks, impacts and outcomes of power disruptions. Fortunately, the duration of most major power outages is hours or minutes, but by looking at what is lost when power is interrupted, it is easier to envision what can happen when these interruptions last for days, weeks, or even months. The Department of Defense (DoD) should learn from these examples.

1859 Carrington white light flare

On September 1, 1859, a noted British solar astronomer, Richard Carrington, was charting sun spot activity when he witnessed a solar event never before observed and recorded by mankind. He noted two intensely bright white spots develop among the dark spots on the surface of the sun. The spots rapidly grew in size and intensity, and then just as rapidly, they diminished and ultimately disappeared. The entire event took less than five minutes.¹

Early the next morning before sunrise, an intense aurora borealis was observed as far south as Cuba.² In addition, telegraph operators reported serious problems with their

¹ Trudy E. Bell and Dr. Tony Phillips, "A Super Solar Flare," *NASA Science: Science News*, posted May 6, 2008, accessed 19 December, 2012, http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/.

² Ibid.

equipment. Some equipment became so overheated the telegraph paper caught fire. Reportedly, one operator received a shock from electricity arcing across several inches of open air. In other, less destructive reports, some operators were able to continue sending and receiving messages even after disconnecting the batteries for their equipment.³ This demonstrates just how much power was being induced in these telegraph lines.

The Carrington white light flare, or Great Carrington Flare, is the largest ever observed and there are not even estimates for what its classification would have been. The most powerful solar flare ever directly measured, an X45 on November 4, 2003,⁴ did not produce a visible light on the surface of the sun like the Carrington white light flare did. Had the Great Carrington Flare occurred within the last few decades, the impact to modern society would have been severe. The consequences of losing the electric grid become more severe as modern life becomes more and more integrated and dependent on electric power. While this, and other, historical examples saw noticeable impacts around the globe, today's reliance on electrical power for essential functions increases the potential effects. This applies to all of society, and has substantial impact on DoD.

DoD's ability to plan, communicate, and execute operations is underpinned by electrical systems. Because of this, the DoD must look at how to mitigate the possibility of not having an electric grid supplying power for periods longer than a few hours or days at most. The current back-up generators lack a sufficient fuel supply to be an alternate source of power on a sustained basis, especially if the rest of the grid out of commission. While refueling a back-up generator may be possible, the source of that fuel has to come

³ Ibid.

⁴ Marusek. This solar flare was measured by satellite systems and while there was an increase in the aurora borealis in conjunction with this event, the CME only grazed the earth so only minor effects were noted in terrestrial systems.

from somewhere. Fuel storage facilities rely on electric pumps. As was seen in Lower Manhattan post-Superstorm Sandy, if these pumps do not have power, the storage tank may as well be empty.

While the possibility of a solar storm of comparable size to the Carrington white light flare is low, the consequences would be dire. Communication and navigation systems would cease to function. Essential services such as waste and water treatment would fail. There would not even be power available for the factories to build replacements for damaged electric grid components. In short, reduction of global society to pre-industrial capabilities would take a matter of minutes.

1989 Solar Storm

On March 10, 1989, a solar event occurred which resulted in a CME that reached Earth in the late evening of March 12. Auroras that night were faintly visible as far south as Florida and Cuba.⁵ At 0244 on March 13, the geomagnetic storm caused by this CME caused a province wide blackout in Quebec, Canada that lasted more than 12 hours.⁶ From the time the first effects started to show up in the grid, it took 90 seconds for the grid to collapse, nowhere enough time for system operators to recognize the impending failure and take actions to limit its effects or prevent it.⁷

In addition to the Quebec grid failure, the North American Electric Reliability Corporation reported widespread impacts to the U.S. and North American power grid that nearly led to large-scale blackouts across major portions of the United States.⁸

Components of the Quebec grid damaged or destroyed included a 1,200-ton capacitor,

⁵ Odenwald. Over 200 power grid problems were reported throughout the United States, but fortunately did not result in grid failures.

⁶ Ibid.

⁷ Radasky and Kappenman.

⁸ Kappenman, docket #AD12-13-000, April 30, 2012.

two step-up transformers, multiple surge arrestors at the La Grande 2 and Churchill Falls generation stations, and a shunt reactor at the Nemiscau substation.⁹

Additionally, the GICs created from this event destroyed a step-up transformer at the Salem Nuclear Generating Plant in New Jersey. The unit cost several million dollars and kept the plant from supplying power anywhere. While the supplier of a new transformer promised to give the replacement order top priority, they stated it would still take almost two years to fill the order. Fortunately, the supplier made a spare transformer available, but this still took six weeks to install and have the power plant back in operation.¹⁰



Figure 2. Step-up transformer damaged at Salem Nuclear Generating Plant due to geomagnetic storm on March 13, 1989. Images provided by Public Service Electric and Gas and taken by Peter Balma (pictured). Photograph on the left shows the outside of the damaged transformer for scale. Photograph on the right shows some of the physical damage to the internal components of the transformer.

⁹ Marusek.

¹⁰ Ibid.

In addition to the terrestrial effects, this X15 class solar storm¹¹ also caused problems with satellites. For several hours, ground stations lost control of several satellites.¹² Had they been communications satellites, DoD headquarters would not have been able to transmit or receive information from deployed units until the satellite recovered, repairs completed, or a replacement launched. While the effects to satellites would greatly compound the problems for DoD in maintaining communications and with navigation and targeting, this kind of vulnerability is beyond the scope of this paper (but does compound electrical power degradation issues).

In the next solar cycle, the largest measured solar flare occurred in 2003. In addition, other measurements used in trace elemental analysis of glaciers show multiple solar storms between four and ten times larger than the March 1989 storm have occurred within the last 150 years.¹³

While there was a great deal learned from the March 1989 storm about procedures that could help prevent similar equipment failures, some of the lessons are now out-dated. During Congressional testimony in 2009, Dr. William Radasky and Mr. John Kappenman stated,

In retrospect, it is also now clear that present U.S. power grid operational procedures are based largely on this out-of-date storm experience, and these procedures will not reduce GIC flows sufficiently; therefore these current procedures are unlikely to be adequate to prevent widespread blackout or damage to key equipment for historically large disturbance events in the future.¹⁴

¹¹ Ibid.

¹² Odenwald.

¹³ Kappenman, docket #AD12-13-000, April 30, 2012.

¹⁴ Radasky and Kappenman.

Once again, the measures taken by electric companies have been deemed sufficient to mitigate risk based on their own analysis; however, the level of risk to DoD capabilities requires further steps to be taken in order to ensure critical capabilities are maintained even during a prolonged power disruption.

DoD must take active measures so that it will be able to generate a sufficient amount of installation energy independent of the civil electric grid. Without an ability to generate electricity on-site, any installation will remain hostage to the vulnerabilities resident in the civil power grid. In addition, any power generation capability must be able to operate without relying on a fuel source provided from external to the installation.

2003 New England Blackout

On August 14, 2003, New England experienced a grid-wide blackout. Among major blackouts, this one was unique in the fact that there was no catastrophic event or violent weather that caused it. Simple negligence or inattentiveness disabled the entire New England power grid through a series of cascading failures. It all started with a power line grounding out on a tree limb that the power company had not adequately trimmed.¹⁵

August 14, 2003, was a hot day and the electrical load on the grid was particularly high. The large amount of power flowing through the lines, and ambient temperature, caused the lines to expand, which resulted in them drooping. At one point, a power line drooped far enough to ground on a tree branch. This caused a cascading system failure affecting 50 million people and covering an area of 9,300 square miles. More than 500 generating units at 265 different plants, including 22 nuclear plants, shut down through

¹⁵ “More Fight – Less Fuel,” 19.

their automated load response systems. While most power restoration occurred within 24 hours, it took nearly 14 days for the New England electric grid generation to regain full capacity.¹⁶

Some may argue that the rapid restoral of power in response to this grid-wide blackout validates that the protection systems already in place work and would be sufficient to respond to other events in the future. However, there is a major flaw in this argument. Restoration of the grid was expeditious because there was no significant damage to any component of the grid.¹⁷ This simple event produced widespread problems. There was no damage to any transformers or generation facilities and there was no major damage to the transmission lines.

Had any of these existed, especially damage to transformers, the blackout likely would have lasted much longer. Restoration of other sections of the grid could have occurred once the damaged component, or components, was isolated. However, this troubleshooting effort to identify the damaged component would have taken more time. Meanwhile, the section fed through the damaged critical component would have remained without power until repair or replacement of that component.

In all, this event shows how a single failure can nearly instantaneously affect an entire electric grid. In a matter of minutes, power was lost from western New York to Maine. Every DoD installation in this region suddenly had to rely on back-up generators and hope that normal power was restored before the fuel supplies were depleted. In this instance, critical functions were able to continue with the use of on-site generators or transferred to unaffected facilities, but the disruption was also relatively short. An oft

¹⁶ Ibid.

¹⁷ Ibid.

spoken axiom within the military is that “Hope is neither a strategy, nor a course of action.” If DoD installations do not actively pursue the capability to generate a sufficient portion of their own power, hope will be the only course of action available should a substantial, widespread outage occur. Exploring other sources of power is required.

CHAPTER 5: POSSIBLE SOURCES OF DISTRIBUTED POWER GENERATION

Threats, Risks, and Realities Need Solutions

In order to become less reliant on the civil electric grid, Department of Defense (DoD) would need to create or install some kind of generation capability either on or adjacent to its many facilities. By having on-site power generation, DoD has the potential to greatly mitigate the vulnerabilities of the electric grid infrastructure through acquiring more direct control over access to the equipment and not being dependent on long-transmission lines and their associated vulnerabilities.

Installation energy consumption accounts for 25 percent of DoD's overall annual energy use and is a significant operational cost.¹ Installation energy is defined as all energy used to power installations including non-tactical vehicles (forklifts, trucks, vans, etc.) not covered by the operational energy definition.² An additional benefit beyond the environmental and economic ones that DoD should not overlook is the reliability and security enhancement these on-site systems can provide for installations and their operations. This makes a strong argument in favor of creating energy generation systems that reduce DoD installation dependence on the civil electric grid in spite of possibly large initial capital investments. The combination of potential risks, threats, and fiscal realities provide a case for DoD to pursue and invest in power production.

¹ Congressional Research Service, Department of Defense Energy Initiative: Background and Issues for Congress, by the Congressional Research Service, August 10, 2012 (Washington, DC: Government Printing Office, 2012) summary page 1. Operational energy in this report is defined as “the energy required for training, moving, and sustaining military forces and weapons platforms for military operations.”

² Ibid.

It is prudent for DoD to explore, invest in and develop several alternate sources for its own power generation. Below are some of the possible sources of electricity production that are either currently available or are very near the capability of utility-scale power production. In some cases, some of the systems are already systems in use at selected DoD facilities. However, these demonstration systems are limited in their number and their primary purpose is as an economic or environmental solution to DoD's energy costs.³ It is prudent to incorporate survivability and continuity of operations along with these fiscal and environmental considerations, as this paper has demonstrated. Several options meet all of these criteria.

Renewable Energy Sources

Solar

Solar energy technology has rapidly improved over the last two decades. Part of the incentive for research and development in solar technology has been the rising cost of petroleum. This research resulted in improvements in both the solar panels themselves and in the methods used to produce them. In fact, the average price per kilowatt of electricity produced through solar power has almost equaled the affordability level of other commercial generation sources.⁴

There are two primary types of solar power systems. The first, called photovoltaic (PV), is the most familiar. Most residential systems used are PV systems and they are scalable for utility level production. The second type is concentrated solar technology. This also comes in two types, concentrated PV (CPV) and concentrating

³ General Charles H. Jacoby, Jr., USA, Commander, USNORTHCOM and NORAD, March 13, 2012, before the Senate Armed Services Committee, 112th Cong. 2nd sess.

⁴ U.S. Energy Information Administration, *Annual Energy Outlook 2012: Levelized Cost of New Generation Resources in the Annual Energy Outlook 2012*, July 12, 2012, accessed February 20, 2013, http://www.eia.gov/forecasts/aeo/electricity_production.

solar power (CSP). CPV uses a lens to focus sunlight on a PV cell and thereby increase the cell's electrical output by focusing the sun's energy on a solar cell. CSP are thermal systems and use mirrors to focus sunlight on a single point. This creates very high temperatures and used to create steam, which in turn powers turbines to generate electricity.⁵ CSP is only a viable option for large, utility scale production. However, scaling PV and CPV systems anywhere from powering calculators to residential needs to utility power is achievable due to their additive capability. This means that in order to get more power from a PV or CPV system, one need only add more panels.⁶

Among PV cells, there are currently two types. The first is the most widely produced and used; crystalline silicon accounts for 80-85 percent of global PV production.⁷ The second type, called thin film due to its manufacturing process, accounts for 10-15 percent of installed PV capacity.⁸ Each type has advantages and detractors.

Silicon wafers are the primary component in fabricating crystalline silicon cells. These wafers are then treated and combined with other layers to give them resilience to weather and to improve their overall electrical efficiency. This process currently requires high-temperature vacuum environments that increase the manufacturing costs to produce these cells. The average efficiency of crystalline silicone PV cells varies depending on the manufacturing process used, but 11-20 percent is the normal range of solar energy reaching the cell and then converted into electricity.⁹

⁵ Congressional Research Service, U.S. Solar Photovoltaic Manufacturing: Industry Trends, Global Competition, Federal Support, by the Congressional Research Service, June 13, 2012 (Washington, DC: Government Printing Office, 2012), 2.

⁶ Ibid.

⁷ Ibid., 5.

⁸ Ibid., 7.

⁹ Ibid.

Manufacturing thin film solar cells is very different. The material used to convert the sun's energy into electricity is a combined solution of several elements. One of the most common combinations is Copper/Indium/Gallium/Selenide, or CIGS. The solution is applied to a substrate, most commonly glass, molybdenum, or other thin metal foils. This process allows thin film cell production to be much faster and cheaper than the crystalline silicon cells. However, the average efficiency of thin film cells ranges from 5-13 percent.¹⁰ However, several companies have achieved efficiencies over 13 percent.¹¹ On September 1st, 2011, the National Renewable Energy Laboratory certified one company's commercial production thin film cell at 17.1 percent efficiency. The record laboratory produced CIGS cell has an efficiency of 19.9 percent.¹² These cells are also much lighter and their useful life spans are equivalent to the crystalline solar cells making them more attractive to installers. The reduced weight means less structural reinforcement required if the panels are roof mounted, and a lower shipping cost due to their lower weight. With lower production costs compared to crystalline cells and the rapid increase in thin-film cell efficiency, the end-customer cost for a solar array of a given power generation will continue to fall.

Given the costs and benefits of these two different PV cells, a DoD installation could look to either in order to provide a possible source of on-site power generation. The crystalline cell panels are more efficient, therefore requiring fewer panels, but the thin-film cell panels are less expensive and lighter allowing their installation on roofs that

¹⁰ Ibid.

¹¹ Chris Whitmore, "Nanosolar's Flexible Foil Technology Achieves 17.1% Aperture Efficiency in NREL Tests," October 6, 2011, accessed December 29, 2012, http://www.pv-tech.org/news/nanosolars_flexible_foil_technology_achieves_17.1_aperture_efficiency_in_nr.

¹² News Release NR-0408 from National Renewable Energy Laboratory, March 24, 2008, accessed December 29, 2012, "Record Makes Thin-Film Solar Cell Competitive with Silicon Efficiency," <http://www.nrel.gov/news/press/2008/574.html>.

crystalline cell panels would be too heavy or expensive, due to additional structural support, to install.

Several DoD installations have installed utility scale PV systems. Three examples include Nellis Air Force Base, NV (14.2 MW array), Naval Station Norfolk, VA (2.1 MW array), and Marine Corps Logistics Base Barstow, CA (approximately 1 MW combined from two arrays). These systems are helping to reduce the dependence of each installation on the civil electric grid while also helping DoD save money on installation energy costs.¹³ In fact, the systems installed at Nellis AFB and MCLB Barstow were funded through a power-purchasing agreement that resulted in no upfront cost to the installation or DoD and purchasing power from these arrays at less than the rates from grid supplied electricity.¹⁴

Using the previously noted initiatives as models, DoD can determine the proper feasibility of solar arrays for supplying installation power in different geographic regions. They also conform to DoD initiatives for building energy generation systems on DoD and other federal land where system construction, financing, and maintenance are the responsibility of the power companies. These systems are designed and installed with the DoD or other federal installations as the primary customer. Any excess energy produced is then available to other grid users.¹⁵ A power generation system like this would insulate

¹³ Martin LaMonica, *CNET.com*, "Air Force Base in Nevada Goes Solar with 14-Megawatt Array," December 5, 2007, accessed December 29, 2012, http://news.cnet.com/8301-11128_3-9829328-54.html; Scott Harper, *The Virginia Pilot, PilotOnline.com*, "Navy Builds Solar Power Farm Near Norfolk Base," December 4, 2012, accessed December 6, 2012, <http://hamptonroads.com/2012/12/navy-builds-solar-power-farm-near-norfolk-base>; Katie Lucia, "MCLB launches new solar farms", *Desert Dispatch*, October 22, 2012, accessed December 17, 2012, <http://www.desertdispatch.com/articles/new-13635-solar-barstow.html>.

¹⁴ Martin; Lucia.

¹⁵ David R. Baker, *San Francisco Chronicle*, "Military Urges Wind, Sun Power for Bases," August 6, 2012, accessed August 7, 2012, <http://www.sfgate.com/business/article/Solar-wind-power-get-Pentagon-boost-3767317.php>.

and provide resiliency for an installation regardless of disruptions from any vector affecting other parts of the electric grid.

Another benefit of PV systems is that they require very little maintenance. Fixed array systems have no moving parts and require no refueling. While many installations do not have wide-open spaces available for use as a solar array location, nearly every building has roof space useable for mounting panels. As a secondary benefit, mounting solar panels on the roof of a building will actually block sunlight from hitting the roof, thereby preventing the roof from heating up as much. This can help to reduce the amount of energy required to cool the building and the equipment inside. The panels generate power any time sunlight is hitting the array.

Conversely, at night these panels will not produce any energy. This can pose the problem of how to store energy for when the sun is not shining. Some solutions in use are battery banks, thermal energy storage, and chemical-thermal systems. All of these add cost and complexity to the overall system. While each storage system has its own benefits and detractors, discussion will focus on only one type of system as a representative example. The individual advantages and disadvantages of every type are beyond the scope of this paper, but suffice it to say that even the ability to have power at least while the sun is shining could greatly enhance an installation's ability to continue its mission.

One type of solar energy storage system does not use PV cells, but is a CSP system that uses liquid salts. The salts are heated using concentrating mirrors, which turn the normally crystalline salt into liquid form. This liquid is in excess of 400 degrees Celsius and creates steam using a heat exchanger. This steam in turn drives a turbine that

actually produces the electricity. This high temperature liquid salt can be stored in tanks for use even after the sun has set.¹⁶

This process obviously adds a great deal of complexity compared to a PV or CPV system in terms of required maintenance for pumps, storage tanks, heat exchangers, and the steam turbines themselves. However, a properly sized system in a conducive geographic location could provide a stable supply of electricity even after the sun sets. With an energy storage system like this, power fluctuations are minimized, useful electricity generation time is extended, and an installation would be more secure in its ability to maintain critical operations. However, with such a system, there would also be an increase in the amount of maintenance required and personnel required to conduct this maintenance. In addition, liquid salt storage systems are only viable in certain geographic areas of the United States due to the solar radiation requirements to make them effective. Therefore, other systems would need to be identified for DoD installations in other parts of the country.

In all, the current state of, and near-term potential advancements in, solar power technology represent a viable opportunity for DoD installations to reduce their dependence on the electric grid, increase survivability and operability during an electric grid failure, and ease both the fiscal and environmental impacts of installation operations. Solar arrays are relatively immune to cyber threats due to their passive energy generation and they would enjoy a relative amount of protection from physical attack due to their location on installation property. If damage occurred to individual panels, the remaining panels would continue to produce power. This would apply also to an EMP event, solar

¹⁶ David Biello, *Scientific American*, "How to Use Solar Energy at Night: Molten Salts Can Store the Sun's Heat During the Day and Provide Power at Night," February 18, 2009, accessed February 20, 2013, <http://www.scientificamerican.com/article.cfm?id=how-to-use-solar-energy-at-night>.

storm, or even terrestrial weather. However, it is possible that a solar array will be unaffected by a solar storm due to their not needed to be connected to end users by high-voltage power lines. This kind of simple operation, low maintenance, and overall survivability make solar power an attractive option for DoD installations in suitable geographic locations.

Wind

As with solar, DoD installations could employ large wind turbines in unused space, or smaller, lower wattage types of wind turbine systems could be mounted on installation rooftops. A brief review of the market for residential or commercial scale wind turbines produces a very large number of available products. These readily available turbine designs have low wind requirements (some start producing power in winds as low as 4-5 miles per hour) and could be very easy to install.

The two main types of wind turbines are horizontal axis and vertical axis wind turbines (HAWT and VAWT). The HAWTs are the most common and are most common for use in utility level electricity production. VAWT have a number of engineering challenges for large size systems such as harmonic resonance at certain wind speeds, bearing load issues, and uneven efficiency over the length of the blades due to low altitude wind generally being slower and more turbulent.

For large, utility-scale wind generation systems, the HAWT currently provides the best solution. However, these systems are very tall, with some towers reaching several

hundred feet with blade lengths over 100 feet.¹⁷ This would obviously present problems at installations with low flying aircraft in the vicinity.

Marine Corps Logistics Base (MCLB) Barstow, CA, has a 1.5 MW HAWT installed in March 2009 and provides approximately 3,000-megawatt hours of power.¹⁸ In conjunction with the recently installed solar arrays, this combination of on-site power generation is capable of providing approximately 25 percent of the installation's annual power requirements.¹⁹ This combined system is a major step towards achieving DoD's policy "to use onsite, self-contained power for critical functions, DoD facilities-based microgrids, and netted area microgrids for extended strategic islanding."²⁰

The second type of wind turbine is the VAWT. While there are a few utility scale VAWTs, the majority of this type are much smaller with blade lengths of only a few feet to a few meters. Primarily purposed for locations where wind is generally present, these systems fit where there is not the room available for a HAWT. One advantage VAWTs have over HAWTs is that they can operate with wind from any direction so there is no requirement to turn the turbine into the wind. Additionally, even though they are individually smaller, installing multiple VAWTs in a distributed area produces a credible amount of electricity. Some possible installation sites are at the corners of buildings, atop poles around parking lots, or anywhere else that receives an appropriate amount of wind.

¹⁷ Eric Rosenbloom, "A Problem with Wind Power," linked table "Size Specifications of Common Industrial Wind Turbines," accessed February 20, 2013, <http://www.aweo.org/windmodels.html>.

¹⁸ News release from NAVFAC Southwest, "First Large Scale Wind Turbine for Marine Corps Commissioned," March 30, 2009, accessed January 10, 2013, https://portal.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_navfacsw_pp/nr_archives_2009/mclb_barstow_windturbine_27mar09.pdf.

¹⁹ King, Huntzinger, and Nguyen, 59. Based on FY08-09 data of all DoD installation average annual power requirements.

²⁰ "More Fight – Less Fuel", 2, citing Department of Defense Instruction 1470.11 §5.2.3.

Rooftop urban settings, with their turbulent and gusty winds, present unique design requirement for which some newly developed VAWT systems are especially suited. One design, installed on an apartment building roof in Hungary and on a tower at Keele University in England, performs as a teaching and test platform.²¹ This 1 kW system optimizes its performance for the turbulent air found near buildings, winds as low as 4 mph, and already has an improved version in design for a 12 kW version of the same dimensions. Expectations are to be able to scale up to megawatt designs.²²

As with a solar system, a detractor to wind generated electricity is that it is not a steady and constantly available generation system. However, energy can be stored. Using a battery bank is the most common method. In Kodiak, Alaska, this is exactly what the Kodiak Electric Association (KEA) has done. As the sole supplier of electricity for Kodiak Island, and several adjacent islands, KEA must produce all of the energy on the island to support the population and businesses. It currently accomplishes this through three sources; two hydroelectric dams, several diesel generators, and six 1.5 MW HAWTs.²³ As the second phase of the wind generation project, KEA increased the number of turbines from three to six at the same time they installed a large battery bank to help store power and provide a more stable supply of electricity.²⁴ As an example of what this has allowed KEA to do, on Thanksgiving Day, 2012, the wind-generated power met 44 percent of the power requirement, and the two hydroelectric dams provided the

²¹ Derek Markham, "New Vertical Axis Wind Turbine Prototype Takes Aim at Urban Wind Power," *treehugger.com*, July 20, 2012, accessed December 17, 2012, <http://www.treehugger.com/wind-technology/new-vertical-axis-wind-turbine-prototype-takes-aim-urban-wind-power.html>.

²² Ibid.

²³ KEA website, accessed December 14, 2012, <http://www.kodiakelectric.com/generation.html>.

²⁴ "KEA Thankful for Renewable Energy Accomplishments," KEA, November 30, 2012, accessed December 14, 2012, <http://www.kodiakelectric.wordpress.com>. First phase was started in 2009 with the installation of three 1.5 MW HAWTs. Phase two was undertaken and completed in fall 2012 with the addition of three more 1.5 MW HAWTs for a total wind generated power of 9 MW.

other 56 percent.²⁵ Because of the amount of renewable power now available to KEA, the need for the diesel generators has reduced dramatically. Since the first wind turbine came on-line in July 2009 until January 2013, KEA has generated 50,671,207 kW of wind power resulting in saving 3,568,395 gallons of diesel fuel.²⁶ If a DoD installation could realize comparable fuel savings, back-up diesel generators could last much longer on their current fuel tanks. This would give much greater flexibility and security to our installations and operations.

Electricity generated by wind turbines of varying design can be an excellent source of power for an installation, but only if proper site surveys are conducted to determine the true output potential in a given geographic location. The example given for Kodiak, Alaska, is a location that is very conducive to generating power through renewable resources. The wet and windy climate produces more than adequate rainfall to keep the reservoirs full and a relatively steady source for the wind turbines to generate power. Obviously, a similar system would not necessarily be effective in a more arid location with less consistent wind patterns. In addition, at installations where low flying aircraft operate regularly, a wind turbine several hundred feet tall at the top of the blades would obviously present hazards that could outweigh the benefits even if the wind environment was appropriate. However, a VAWT such as the one previously described may be suitable at these installations due to not creating any significant obstruction to flight operations. All installations, not just those with large open spaces that do not have associated air operations, should conduct surveys to determine whether wind turbine systems would be appropriate.

²⁵ Ibid.

²⁶ KEA website, accessed February 12, 2013, <http://www.kodiakelectric.com/generation.html>.

In terms of survivability or vulnerability to the previously described threat vectors, wind turbines fair relatively well. HAWTs basic structure is makes it vulnerable to physical attack; however, placing these turbines on DoD installations will add a layer of protection against this threat vector with no added burden to security forces in maintaining the integrity of the installation boundaries. VAWTs have a slightly increased advantage over HAWTs in surviving physical attack partly because they are smaller and attract less notice. Unlike HAWTs, installing VAWTs in close proximity to existing structures is possible, thereby lending the additional benefit of observing perpetrators before they can carry out their attack.

Cyber-attacks and EMP events could be a problem for the large HAWTs due to their monitoring systems and controls necessary to keep the turbine pointed into the wind and blade angles appropriately set for the wind conditions. Meanwhile, solar storms should not present major issues for wind turbines of either design for the same reason solar arrays remain generally insulated, short distances to the end user negates the need for high-voltage transmission lines.

Terrestrial weather, except in the most extreme situations such as category V hurricanes, does not present any major obstacles to the use of wind turbines. Large HAWTs are in use around the world in offshore “wind farms” in locations as tempestuous as the North Sea. If they can survive such a harsh environment as that, then the environments of most DoD installations should be well within the structure design capabilities of existing models.

Non-renewable Energy Sources

While a renewable resource is an attractive possible solution to providing a long-term power supply for DoD installations, their ability to provide a constant and always available source of electricity is a problem. This is one reason why these technologies have been slow in their widespread adoption. Using non-renewable resources such as coal, natural gas, and petroleum allows for more stable electricity generation. However, these generation systems also require a steady supply of their fuel in order to continue functioning. This supply dependence is a vulnerability during long-term, widespread power outages because “transportation systems would be at a standstill with no power to pump the fuels.”²⁷ As witnessed in lower Manhattan in the aftermath of Superstorm Sandy, back-up generators ran out of fuel within hours or at most a few days.²⁸ Like the Manhattan hospital generator that 30 National Guardsmen were tasked with keeping fueled,²⁹ some DoD operations are continuous and cannot risk interruptions in power.

While keeping this refueling issue in mind, two possible solutions for providing on-site power generation for DoD installations are hydrogen fuel cells and small modular reactors (SMR).

Hydrogen Fuel Cells

Hydrogen fuel cells have a broad range of uses. Current fuel cell usage ranges in size and output from batteries for deployed troops to back-up power and full power

²⁷ Gilbert.

²⁸ Shachtman.

²⁹ Ibid.

supply for buildings.³⁰ Fuel cell basic operating principles are the recombination of hydrogen and oxygen across a conductive catalyst resulting in electricity, heat, and water.

There are a number of varying designs based on this general premise. Some fuel cells use a supply of natural gas, while others operate mainly off a pure supply of hydrogen. For the purposes of this discussion, this paper will focus on the use of hydrogen only due to the recommendation of supplying on-site power generation without off-installation resources.

Before discussing possible on-site sources of hydrogen, this paper describes current fuel cell capabilities. As stated before, hydrogen fuel cells recombine hydrogen and oxygen in order to produce electricity. The two by-products of this hydrogen only fueled reaction are heat and water. In systems that use natural gas as a fuel source, other exhaust products result as well. The hydrocarbon chemical chains in natural gas go through a reforming process that separates the hydrogen from the rest of the hydrocarbon chain. This results primarily in byproducts of carbon dioxide, nitrogen-oxides, and trace amounts of carbon monoxide; however, these exhaust products are produced at a much lower rate than would be produced by using the natural gas in combustion.³¹ However, for hydrogen only fueled cells, these exhaust chemicals are not present. Therefore, it simplifies the fuel cell maintenance and design by not having multiple waste products to deal with.

³⁰ Department of Defense, Defense Logistics Agency, *Beyond Demonstration: The Role of Fuel Cells in DoD's Energy Strategy*, by Thomas J. Gross, Albert J. Poche, Jr., and Kevin C. Ennis, Defense Logistics Agency Research & Development (October 19, 2011), 7.

³¹ "Environmental Technology Verification (EVT) Program Case Studies: Demonstrating Program Outcomes Volume II," (National Risk Management Research Laboratory, Office of Research and Development, U.S. Environmental Protection Agency, September 2006) 34-37.

Harnessing the water and waste heat from a hydrogen-supply only fuel cell can increase the efficiency of the overall system. Fuel cells installed for powering buildings can also provide for infrastructure heating (spaces, water, and process heating) in systems called Combined Heat and Power (CHP) systems. By harnessing the heat generated within the fuel cell, installed systems achieve efficiencies of greater than 80 percent.³² Obviously, this kind of CHP system can also help reduce a building or installation's overall energy requirement. For many installations, if multiple fuel cell farms were combined, they could provide enough power and infrastructure heating to supply 100 percent of the installation power requirements and have excess available to provide outward into a surrounding community's electric grid. Distributing fuel cells throughout an installation would also help create redundancy and survivability, allowing a more flexible response during the limited maintenance requirements or during a grid-power outage.

Multiple DoD installations are already conducting test installations of hydrogen fuel cells to supply back-up power for individual buildings while some commercial entities have installed systems large enough to provide everyday normal power as an offset for grid-supplied electricity.³³ These initiatives, along with improvements in the research and production of new hydrogen fuel cells, have had, and are having, dramatic effects on reducing the cost of hydrogen fuel cells. Analysis by the Battelle Memorial Institute for the U.S. Department of Energy in 2011 concluded that the "2015 cost of a 5-kW fuel cell system for backup power applications could be about 60 percent of the 2010

³² "Beyond Demonstration: The Role of Fuel Cells in DoD's Energy Strategy," 11.

³³ Ibid., 11-14.

cost.”³⁴ This dramatic reduction in up-front price, coupled with lower operating and maintenance costs can result in large savings over the lifetime of the system when compared to standard diesel powered backup generators used today. In fact, according to one manufacturer, even if a fuel cell system’s first-cost estimate is 20 percent higher than a comparable output diesel-generator system, fuel cell economics will still be superior due to longer life spans, lower maintenance costs, and lower greenhouse gas emissions.³⁵

Additionally, fuel cells are capable of providing steady, stable power as long as their fuel source lasts. In some locations, it may be possible to use renewable energy sources such as wind and solar to power hydrogen generators thereby creating hydrogen on-site and not requiring supply from off the installation. As an example, the City of Hempstead, New York, is using a 100-kW wind turbine to power a water-to-hydrogen generator for use in the city’s vehicle fleet. Excess electricity from the wind turbine feeds into the grid.³⁶ DoD installations could use this concept to generate hydrogen where it could be stored or used immediately. The source of the hydrogen is water. The water feeds into an electrolyzer, which separates the hydrogen from the oxygen producing pure hydrogen and oxygen gas. While most commercial systems require a supply of treated fresh water, the U.S. Naval Research Laboratory has been developing a system that uses seawater.³⁷ For installations located near the oceans, this capability could be exploited to power fuel cells without affecting, or relying on, fresh water supplies. This

³⁴ Ibid., 9.

³⁵ Ibid., 29.

³⁶ News release from Town of Hempstead, Long Island, NY, “Town’s Answer to Clean Energy is Blowin’ in the Wind: New Wind Turbine Powers Hydrogen Car Fuel Station,” December 12, 2011, accessed November 25, 2012, <http://www.townofhempstead.org/news/564-towns-answer-to-clean-energy-is-blowin-in-the-wind-new-wind-turbine-powers-hydrogen-car-fuel-station>.

³⁷ Mike Hoffman, “Converting Sea Water to Navy Jet Fuel,” *Military.com*, October 2, 2012, accessed January 7, 2013, <http://defensetech.org/2012/10/02/converting-sea-water-to-navy-jet-fuel/>.

technology would likely be particularly suitable for U.S. Navy installations due to location.

By using hydrogen fuel cells, the opportunity exists to maintain a stable power supply with a very high efficiency rating when integrated into a CHP system. This could actually help reduce the amount of power required for the installation overall. In addition, the capability exists to create the fuel on-site without reliance on an external supplier. The primary risk in using hydrogen fuel cells is the reliance on a steady supply of hydrogen. Just as with diesel generators, without fuel, hydrogen fuel cells will not produce any power. However, unlike diesel generators, there are commercially available systems capable of generating hydrogen on-site, thus eliminating or greatly reducing the risk of loss of power due to lack of fuel.

Hydrogen fuel cells have many of the same survivability and protection attributes as diesel generators. They are located near the end user and require little in the way of computerized control systems, which lowers the cyber-attack threat. In terms of solar or terrestrial storms, they would be no more at risk than the buildings they would power. An EMP event could result in damage or destruction of the working components, but mitigating this threat through simple design additions when building the hydrogen fuel cell power plant is well within the technical and economic realm of possibility.

Small Modular Reactors (SMR)

Another potential but less common or well-known solution resides in the small nuclear reactor realm. The International Atomic Energy Agency classifies any reactor producing 300-MW or less as Small Modular Reactors.³⁸ While there are significant

³⁸ King, Huntzinger, and Nguyen, 3.

factors to address before trying to locate a nuclear reactor of any type or size, military installations in many cases offer solutions to several issues. By locating a SMR on a DoD installation, a level of physical security is already inherent in the ability to restrict the personnel who would have access to approach the physical plant. Additionally, there are many installations with land located far enough away from civil structures and populations to address safe area issues. However, another consideration that would have to be addressed is the impact to an installation's mission should the installation be required to evacuate in the event of a nuclear incident. If the result of this kind of evacuation would create lasting damage to national security, then SMR would certainly not be a viable option.³⁹ However, this does not mean that nuclear power can never be an option for DoD installations. In 1963, Southern California Edison Corporation acquired an easement to operate a nuclear reactor on Camp Pendleton MCB. To date, there have been no significant impacts on the training or readiness of the installation or the units stationed there.⁴⁰ Therefore, with thorough survey and site study, there may be more DoD installations that could be ideally suited to host a SMR.

There are currently several companies from around the world that are working on the design and approval of various sized SMRs.⁴¹ Some have design outputs as small as 10 MW, while others have design outputs exceeding slightly more than 300 MW.⁴² This high end far exceeds the current energy requirements of any DoD installation in the world. As a recent government report stated, a SMR of 160 MW or smaller "could

³⁹ Ibid., 37.

⁴⁰ Ibid.

⁴¹ Ibid., 6-9.

⁴² Ibid, Table 1, 9.

supply the average energy usage by any military installation.”⁴³ Based on the 2008-2009 energy usage reported by U.S. military installations, a 45 MW generation system satisfies the power requirements for 90 percent of installations, and 80 percent of installations could fully meet their average electricity usage from a plant generating 35 MW.⁴⁴

Nuclear reactors must be considered a source of non-renewable energy since they consume their fuel source. However, each planned fueling for a nuclear reactor lasts for years, not hours or days. Normal refueling periodicity of large nuclear reactors used for utility electricity production is between 1.5 – 2 years.⁴⁵ Of current SMRs under design, the refuel timeframes proposed are from 1.5 to 30 years depending on the design.⁴⁶ This inherent ability to provide stable power for very long periods can make them an attractive solution to providing DoD installations with consistent, reliable power independent of the civil power grid.

Like any other high-capacity power generation facility, nuclear power plants are expensive to build. The large plants currently utilized for grid power recoup their costs due to their long life spans and infrequent refueling requirements. SMRs would also capitalize on the capability to build the primary reactor vessel at a factory and then deliver it in a plug-and-play configuration via either truck or rail. This would also greatly reduce on-site construction time and costs. Companies utilizing recognized production method efficiencies in a factory setting while building these reactors will reduce design and assembly costs.⁴⁷ For DoD installations, this means a significantly shorter time from

⁴³ Ibid., 14. This statement was based on the reported FY08-09 energy useage of U.S. military installations.

⁴⁴ Ibid., Figure 3, 23.

⁴⁵ Ibid., 5.

⁴⁶ Ibid., Table 2, 9.

⁴⁷ Ibid., 4-6.

beginning of construction to initial operation and achievement of reducing strategic and operational risk to an installation's mission capability. An objective measure of this reduced construction time is not available because SMRs are still in the design and certification process.

As designs mature, the U.S. Nuclear Regulatory Commission (NRC) must review and certify systems for safety and reliability. As of 2011, two advanced SMR designs were nearing completion and had received extensive NRC design review.⁴⁸ In November 2012, the U.S. Department of Energy announced that it had awarded project support funding for the design, license, and commercialization of a SMR design by Babcock & Wilcox.⁴⁹ The proposed SMR expects to have a 125 MW capacity with a five year refuel period.⁵⁰ This size plant could provide 100 percent of the average annual power requirement for better than 95 percent of military installations.⁵¹

With industry moving forward and the Department of Energy helping to bring SMRs to a commercial production capability, the economics of a reactor like this could be within the realm of possibility for the DoD. However, if DoD would have to take on the costs of first of a kind (FOAK) designs, the additional cost would greatly outweigh any benefits received. As of 2011, the national retail average for electricity was 10.3 cents per kilowatt-hour.⁵² Excluding FOAK costs, the average estimate of SMR supplied

⁴⁸ Ibid., 7.

⁴⁹ News release from U.S. Department of Energy, "Energy Department Announces New Investment in U.S. Small Modular Reactor Design and Commercialization," November 20, 2012, accessed November 23, 2012, <http://energy.gov/articles/energy-department-announces-new-investment-us-small-modular-reactor-design-and>.

⁵⁰ King, Huntzinger, and Nguyen, Table 1, 9.

⁵¹ Ibid., Figure 3, 23.

⁵² U.S. Energy Information Administration, *Average Retail Price of Electricity to Ultimate Customers by End-Use Sector, by State, September 2012 and 2011*, accessed November 25, 2012, http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_06_a.

power would be 8 cents per kilowatt-hour.⁵³ Coupled with the possibility of using a Purchase Power Agreement where a power company assumes the construction and operation costs such as was used for the solar array at MCLB Barstow, SMRs may be a very economically attractive alternative for DoD.

SMRs could also provide an additional capability for DoD installations. The waste heat generated and left over from electricity production can be used for other purposes. One suggested capability is the ability to generate transportation fuels such as various bio-fuels and coal-to-liquid conversion processes using coal and natural gas.⁵⁴ While this capability would most likely not be available to be exploited during an extended grid power outage due to a break down in civil transportation systems, the supplies on hand may be enough to help generate fuels long enough to help transport critical personnel and equipment to unaffected areas.

All nuclear facilities have requirements for physical security that exceeds those required for a non-nuclear power plant for several reasons. One obvious requirement is to maintain positive control of the nuclear material as a matter of national security. The security already in place restricting access to a DoD installation could meet some of the requirements that factor into the construction of nuclear plants. This layer of security well beyond the physical premises of the SMR could definitely be beneficial in helping to prevent a successful physical attack just by adding distance from unrestricted public areas to the reactor itself.

For the staffing and maintenance of a SMR, the U.S. military already has personnel and programs for training and operating nuclear reactors. Augmenting the U.S.

⁵³ King, Huntzinger, and Nguyen, 15.

⁵⁴ Ibid., 27.

Navy's nuclear training program to provide a source of trained and experienced personnel to meet the increased personnel demand created is one possibility. While the programs for training and active duty tours would need to be increased and/or modified to produce a larger qualified workforce, this would not be beyond the realm of possibility. It is possible to achieve the increase in qualified personnel in a relatively short period.

Another possible source of operators for these new SMRs could be personnel separating from the military that already have the qualifications and experience of running nuclear reactors.

Public opinion is one other issue requiring address before the construction and utilization of a nuclear reactor. There are many influences that affect this important issue that are beyond the scope of this paper, but safety and the storage and disposal of spent fuel will be two large factors. With using smaller amounts of fuel and refueling taking place at longer intervals, each plant would actually generate less spent fuel than current nuclear power plant designs. An educational communications plan focusing on the safety and benefits of SMRs would be necessary and may be able to address some of the public's concerns. It may be possible to determine initial public sentiment and feelings on this issue by surveying the existing power companies to find out if they have conducted any type of public opinion survey on this issue. Some areas of the country, and especially at overseas installations, may never be accepting of having a nuclear plant of any size.

While SMRs are still in the developmental phase, their existence and benefits are rapidly approaching. The ability of a DoD installation to generate all of its power requirements on a continuous basis regardless of the electric grid beyond the fence line

would eliminate most of the vulnerabilities associated with the civil electric grid. With the generation source so close to the end user, there would not be a need to step-up the voltage for long-distance transmission thereby reducing another vulnerability.

Additionally, with most draft designs capable of exceeding a significant percentage of DoD installation power requirements, a SMR could help mitigate the effects to the surrounding community from major grid failures.

If it is determined that a SMR should be constructed on a DoD installation, the survivability of the facility would be greatly enhanced by the mere fact that it is on a DoD installation. The restricted access environment provided would create an additional layer of security beyond that already established around current nuclear power facilities. Coupled with the inherent durability of large power generation facilities, SMRs would be well insulated against all but the most determined threat. It would even provide the host installation an additionally increased level of resilience by negating some of the possible threat vectors due to proximity and not needing long-distance transmission lines or major step up and step down transformers. In all, a DoD installation with a resident SMR would enjoy a very high level of capability to continue installation operations for very long periods regardless of the status of the civil electric grid.

CHAPTER 6: CONCLUSIONS

The existing civil electric grid that Department of Defense (DoD) installations depend on to carry out their missions is fragile and vulnerable to a variety of disruptions. With more than 6,000 utility generation units, more than 500,000 miles of high power transmission line, and approximately 12,000 major substations for the step up of voltages for transmission and step down for end use, this paper has shown the possibility for grid disruptions is very real and significant. Critical system elements can be easily targeted and disrupted or destroyed. These disruptions can lead to grid system failures lasting days, weeks, months, even years if certain components require building replacements due to damage or destruction.¹ The impact of this could be the inability of combatant commanders or other critical headquarters to exercise command and control with subordinate units, deploy forces, conduct planning efforts, or communicate coordinating instructions to deployed units.

Current measures at most DoD installations are inadequate to mitigate the effects of long-term power outages. Most have back-up generators capable of powering a single building, or often just parts of a single building, typically with a fuel supply for less than five days.² While this may be acceptable for temporary power interruptions regularly experienced from minor weather system effects, this solution does not materially decrease the installation's dependence on the civil electric grid. If a power disruption lasts longer than the fuel capacity of an installation's back-up generator, that installation

¹ "More Fight – Less Fuel", 55.

² King, Huntzinger, and Nguyen, 25.

could be considered a “soft-kill” until such time as power is restored. The opportunity presented to an adversary in such a situation could prove to be catastrophic.

The economics of an on-site power generation system, while important, need not be the limiting factor in moving forward with an aggressive program of lowering DoD installation reliance on the civil electric grid. As demonstrated at several installations already, the DoD can have systems designed, built, and placed in operation with no up-front costs to DoD using Power Purchase Agreements (PPA). This method must be afforded more consideration given the savings that can be realized once a project becomes operational and the benefits to continuity of operations in the event of electric grid disruption.

Over the period from 2000 to 2010, the average price of electricity has gone up from 6.81 cents per kilowatt-hour to 9.83 cents per kilowatt-hour.³ This kind of increase can be expected to continue in the future and will complicate DoD’s budgeting capacities as much as it impacts business and others, if not more. If DoD installations move forward with constructing on-site power generation capabilities through PPAs with fixed rate agreements, even a system with a cost a few cents more than the current retail price could reach parity within a few years and as a near certainty within the systems lifespan. DoD agencies have been hamstrung in the past by the budget process for systems that will reach their economic benefit outside of the current budget cycle. If PPAs are not available for some projects, consideration of lifecycle cost savings should be prominent in determining the feasibility of committing to these projects.

³ U.S. Energy Information Administration, *Average Retail Price of Electricity to Ultimate Customers by End-Use Sector, 1999 through 2010 (cents per kilowatt hour)* Electric Power Annual 2010 Data Tables, Table 7.4, November 9, 2011, accessed December 29, 2012, <http://www.eia.gov/electricity/annual/html/table7.4.cfm>.

Assistant Secretary of the Air Force (Installations, Environment, and Logistics)

Terry Yonkers noted such budgetary limitations in planning and budgeting at a 2012 conference on military energy challenges,

The other dimension of this is the payback. And so we think in terms of five years and some of the discussions we're having across the board is, if we make smart investments, it will take about ten or eleven years to hit the breakeven point. But after that point in time, we'll save a billion and a half or more dollars, once we get into sort of the full production and the modification.⁴

In addition, energy prices alone should not be the deciding factor. DoD must consider the increase in security provided for installations and missions by creating a level of long-term energy independence from the civil electric grid.⁵ Otherwise, DoD is overlooking a major benefit of having and using on-site electricity generation.

Commercially available systems have reached a point where they can provide power at competitive economic rates. As well, the longevity, efficiency, and maintainability of many of these systems make them excellent options to replace current diesel back-up generators that have limited fuel supplies, require relatively large amounts of maintenance, and used only in case of emergency.

All of the previously addressed systems, solar, wind, hydrogen fuel cells, and SMRs, have advantages over diesel generators in their longevity. Solar and wind, while not suitable in every location due to environmental factors, require little maintenance and have an inexhaustible, though inconsistent, source of fuel. However, the sun is not always shining and the wind is not always blowing. Through prudent combinations of systems, augmenting the times where these renewable energy sources are not producing

⁴ Gary Roughead, ADM, USN(Ret), Jeremy Carl, and Manuel Hernandez, LCDR, USN, "Powering the Armed Forces: Meeting the Military's Energy Challenges," Hoover Institution Press, Stanford University, Stanford, CA, Hoover Institution Press Publication No. 628, Copyright 2012, 41.

⁵ Gross, 8.

power via other power generation methods is possible. Hydrogen fuel cells require very little maintenance, can integrate into an installation's infrastructure heating in CHP systems achieving very high efficiencies, and can have fuel produced on location via renewable energy sources. SMRs would incur a large maintenance requirement, but they could be capable of supplying 100 percent of an installation's power requirement for several years rather than a single building for a few hours or days.

The emphasis to create these systems need not fall upon the individual installation commander alone. Annually, Functional Combatant Commanders are required to submit a list of infrastructure requirements necessary for mission execution. This list must include a prioritization of required improvements over the five-year future years defense program.⁶ In addition, each Geographic Combatant Commander (GCC) must identify and prioritize critical infrastructure to reduce vulnerabilities that could affect mission accomplishment. GCCs are authorized to work with host nations, commercial entities, the U.S. Department of State and other government agencies to reduce their infrastructure vulnerabilities.⁷ As the Functional and Geographic Combatant Commanders arguably are responsible for the greatest strategic and operational command and control requirements, their emphasis on reducing installation dependence on the civil electric grid could provide the greatest impetus to a system's funding and implementation. These requirements and authorizations can give great weight and opportunity for every installation to explore options appropriate for their location and needs.

⁶ U.S. Joint Chiefs of Staff, *2010 Joint Strategic Capabilities Plan*, Chairman of the Joint Chiefs of Staff Instruction 3110.01H (Washington, DC: Joint Chiefs of Staff, June 10, 2011), Encl. F, F-7, para. 15.

⁷ *Ibid.*, Encl. F, F-4, para. 8.

Civil electricity providers will be reluctant to take measures on their own to create grids that are more resilient because of the costs involved and the impetus to maximize profits within the limits allowed by government. This means that the Department of Defense must take on the responsibility of acquiring the capability to generate electricity for its installations independent of the civil grid's operational status. However, this does not mean DoD must take on the cost of installation and maintenance of these generation systems. A few DoD installations have already executed the construction of on-site power generation through Power Purchase Agreements that cost the DoD nothing up front and actually resulted in fixed rate agreements at rates less than what would normally be paid for grid supplied power. However, the civil electricity providers, with the possibility of a few exceptions, are not going to do this of their own volition.

The capability for DoD to increase its surety of continuous operations in spite of civil electric grid outages exists today. Technology advances in solar power collection and efficiency, wind turbine design, energy storage, hydrogen production, and fuel cell efficiency put power generation sources not reliant on petroleum or coal at comparative economic levels. Advances nearing commercialization in all of these areas will only generate more and better options. A SMR would practically eliminate the need for a connection to the civil electric grid for most installations. All of these options may be able to become operational with zero upfront cost to DoD and reduce installation power costs while simultaneously creating a substantially more secure command and control network in light of the wide range of potential risks to the power grid.

The threats to the civil electric grid are real. Each previously identified threat has happened before and will happen again. The DoD is fortunate that it has not suffered

from a widespread, long duration grid outage, but as financial institutions are fond of putting in small print, past performance is not an accurate indicator of future potential. DoD has the opportunity to create an insurance policy that will not only insulate it from these disasters but will also provide some fiscal relief at the same time.

CHAPTER 7: RECOMMENDATIONS

The U.S. Department of Defense (DoD) should have each installation conduct surveys into the most appropriate types of on-installation power generation capability based on their geographic location, environmental factors, space available, and any operational limitations such as flight operations. These installations should also survey their tenant commands to validate which functions are required to maintain strategic and operational capabilities. This will help confirm which buildings and power systems within those buildings be prioritized to maintain power during an extended grid outage.

Given the constrained fiscal environment that the DoD must operate within over the foreseeable future, it would be advantageous to act aggressively in the acquisition of a program of on-site power generation. Using Power Purchase Agreements and other financial vehicles, the upfront costs to DoD can be minimal or eliminated while realizing near-immediate cost savings in installation power expenditures and an increase in reliability and security of critical mission capabilities.

Combining generation systems could offset each system's short falls. As is already in use by the City of Hempstead, a renewable energy generator such as solar or wind could provide power for a hydrogen generator. This in turn would provide fuel for a hydrogen fuel cell that would provide stable power to the installation identified critical systems. Any excess power produced by the renewable energy source would then be available for the wider installation grid or even the civil grid.

Integrating smaller distributed generators such as rooftop mounted solar panels and smaller wind turbines into an installation's overall energy security plan is necessary even while using large-scale energy production systems. Feeding small systems directly

into non-critical components reduces the overall draw on larger systems. Additionally, connecting these individually small components into micro-grids can result in significant power generation.

While companies developing SMRs complete their designs and gain certification from the U.S. Nuclear Regulatory Commission, DoD should begin to identify installations that have the available land to install SMRs. Public opinion regarding the construction of a SMR could be determined at the same time personnel staffing issues are resolved. This will reduce the amount of time from SMR commercialization to the completion of installation and entry into operational service at appropriate locations.

DoD has the opportunity now to greatly reduce a critical vulnerability. Not to do so is to accept an unnecessary level of risk. As a secondary benefit, the demand placed on the civil infrastructure can be reduced by DoD installations generating a portion of their own power. This would help to increase the capacity – demand gap and could aid in mitigating the effects of losing certain critical grid components.

The U.S. Department of Defense is at an opportune period in time. Technological advances are granting the opportunity for installations to become more self-reliant and secure in their energy requirements at the same time that fiscal pressures demand a reduction in operating costs. Both of these are achievable through aggressively pursuing on-site electric generation capabilities. Every DoD installation should be capable of withstanding a long-term electric grid interruption by generating at least 30 percent of its own power requirements for three weeks without the use of off-installation resources. This capability exists now. Through a considered and aggressive program using solutions, and combinations of solutions, described previously in this paper, DoD can rig

for dark and will be prepared to continue its mission of protecting the country, regardless of the risk on the horizon.

BIBLIOGRAPHY

- Asa, Norman, via PR Newswire, “Cyberattacks on Iran – Stuxnet and Flame.” *The New York Times* via *PR Newswire*.
http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html (August 9, 2012, accessed December 17, 2012).
- Baker, David R. “Military Urges Wind, Sun Power for Bases.” *San Francisco Chronicle*. <http://www.sfgate.com/business/article/Solar-wind-power-get-Pentagon-boost-3767317.php> (accessed August 7, 2012).
- Barrett, Michael. *Ensuring the Resilience of the U.S. Electrical Grid; Part III: Requirements for a More Resilient System*. Arlington, VA: Lexington Institute, November, 2012.
- Bell, Trudy E. and Dr. Tony Phillips. “A Super Solar Flare.” *NASA Science: Science News*. May 6, 2008. http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/ (accessed 19 December, 2012).
- Biello, David. “How to Use Solar Energy at Night: Molten Salts Can Store the Sun’s Heat During the Day and Provide Power at Night.” *Scientific American*.
<http://www.scientificamerican.com/article.cfm?id=how-to-use-solar-energy-at-night> (accessed February 20, 2013).
- Congressional Research Service. *Department of Defense Energy Initiative: Background and Issues for Congress*. By Moshe Schwartz, Katherine Blakeley, and Ronald O’Rourke. Washington, DC: Government Printing Office, August 10, 2012.
- Congressional Research Service. *U.S. Solar Photovoltaic Manufacturing: Industry Trends, Global Competition, Federal Support*. By Michaela D. Platzer. Washington, DC: June 13, 2012.
- Cosmicopia. “The Sun’s Magnetic Field.” National Aeronautics and Space Administration. <http://helios.gsfc.nasa.gov/solarmag.html> (accessed December 19, 2012).
- CQ Transcripts. *CQ.com*. <http://cq.com/transcripts/newsmaker.0> (accessed February 20, 2013).
- Grossman, Elaine M. “Effects-based Operations Under Fire: A Top Commander Acts to Defuse Military Angst on Combat Approach.” *Inside the Pentagon*, April 20, 2006.
- Hammes, Thomas X., COL, USMC, *The Sling and the Stone: On War in the 21st Century*. Minneapolis, MN: Zenith Press, 2004.

- Harper, Scott. "Navy Builds Solar Power Farm Near Norfolk Base." *The Virginia Pilot, PilotOnline.com*. <http://hamptonroads.com/2012/12/navy-builds-solar-power-farm-near-norfolk-base> (accessed December 6, 2012).
- Hoffman, Mike. "Converting Sea Water to Navy Jet Fuel." *Military.com*. <http://defensetech.org/2012/10/02/converting-sea-water-to-navy-jet-fuel/> (accessed January 7, 2013).
- Kodiak Electric Association. "KEA Thankful for Renewable Energy Accomplishments." News release. <http://www.kodiakelectric.wordpress.com> (accessed December 14, 2012).
- LaMonica, Martin. "Air Force Base in Nevada Goes Solar with 14-Megawatt Array." *CNET.com*. http://news.cnet.com/8301-11128_3-9829328-54.html (accessed December 29, 2012).
- Lucia, Katie. "MCLB launches new solar farms." *Desert Dispatch*. <http://www.desertdispatch.com/articles/new-13635-solar-barstow.html> (accessed December 17, 2012).
- Markham, Derek. "New Vertical Axis Wind Turbine Prototype Takes Aim at Urban Wind Power." *treehugger.com*. <http://www.treehugger.com/wind-technology/new-vertical-axis-wind-turbine-prototype-takes-aim-urban-wind-power.html> (accessed December 17, 2012).
- Marusek, James A. "Solar Storm Threat Analysis." *Impact* (2007). , <http://www.breadandbutter-science.com/SSTA.pdf> (accessed September 4, 2012).
- National Renewable Energy Laboratory. "Record Makes Thin-Film Solar Cell Competitive with Silicon Efficiency." News Release NR-0408. <http://www.nrel.gov/news/press/2008/574.html> (accessed December 29, 2012).
- NAVFAC Southwest. "First Large Scale Wind Turbine for Marine Corps Commissioned." News release. https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_navfacsw_pp/nr_archives_2009/mclb_barstow_windturbine_27mar09.pdf (accessed January 10, 2013).
- Odenwald, Dr. Sten. "NASA – The Day the Sun Brought Darkness." National Aeronautics and Space Administration. http://www.nasa.gov/topics/earth/features/sun_darkness_prt.htm (accessed August 12, 2012).
- Office of the President of the United States. President's Information Technology Advisory Committee. *Cyber Security: A Crisis of Prioritization report to the President*. Washington, DC, February 2005.

- Prepared testimony of John Kappenman, , before the U.S. Federal Energy Regulatory Commission at the *Technical Conference on Geomagnetic Disturbances on the Bulk Power System*, docket #AD12-13-000, on April 30, 2012.
- Prepared testimony of Dr. William Radasky, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, with Mr. John Kappenman. 111th Cong., 1st sess., July 21, 2009.
- Rosenbloom, Eric. “A Problem with Wind Power,” linked table “Size Specifications of Common Industrial Wind Turbines.” <http://www.aweo.org/windmodels.html> (accessed February 20, 2013).
- Roughead, Gary, ADM, USN(Ret), Jeremy Carl, and Manuel Hernandez, LCDR, USN. “Powering the Armed Forces: Meeting the Military’s Energy Challenges.” Hoover Institution Press. Stanford University, Stanford, CA: Hoover Institution Press Publication No. 628, Copyright 2012.
- Sanger, David E. and Eric Schmitt. “Rise is Seen in Cyberattacks Targeting U.S. Infrastructure.” The New York Times. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?ref=stuxnet&_r=0 (accessed December 17, 2012).
- Shachtman, Noah. “How Victoria’s Secret Saved the National Guard During Hurricane Sandy”. *Wired.com*. November 2, 2012. <http://www.wired.com/dangerroom/2012/11/victorias-secret-sandy/> (accessed December 19, 2012).
- Stark, Holger. “Mossad’s Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War.” *Spiegel Online International*. <http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-or-cyber-war-a-778912.html> (August 8, 2011, accessed December 17, 2012).
- Testimony of Paul H. Gilbert, before the Committee on House Homeland Security Subcommittee on Infrastructure and Border Security. 108th Cong., 1st sess., on September 4, 2003.
- Testimony of William Graham, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong., 1st sess., on July 21, 2009.
- Testimony of General Charles H. Jacoby, Jr., USA, Commander, USNORTHCOM and NORAD, before the Senate Armed Services Committee. 112th Cong., 2nd sess., March 13, 2012.
- Testimony of Congressman James R. Langevin (D-RI), before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. 110th Cong., 1st sess., October 17, 2007.

- Testimony of Director Joe McClelland, before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. 111th Cong., 1st sess., July 21, 2009.
- Testimony of Chairman Bennie G. Thompson (D-MS), before the Committee on House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. 111th Cong., 1st sess., July 21, 2009.
- Town of Hempstead, Long Island, NY. “Town’s Answer to Clean Energy is Blowin’ in the Wind: New Wind Turbine Powers Hydrogen Car Fuel Station.” News release. <http://www.townofhempstead.org/news/564-towns-answer-to-clean-energy-is-blowin-in-the-wind-new-wind-turbine-powers-hydrogen-car-fuel-station> (accessed November 25, 2012).
- Undersecretary of Defense for Acquisition, Technology, and Logistics. Defense Science Board Task Force on DoD Energy Strategy. *More Fight – Less Fuel*. Washington, DC: Department of Defense, February, 2008.
- U.S. Department of Defense. Defense Logistics Agency Research & Development. *Beyond Demonstration: The Role of Fuel Cells in DoD’s Energy Strategy*, by Thomas J. Gross, Albert J. Poche, Jr., and Kevin C. Ennis. Defense Logistics Agency, October 19, 2011.
- U.S. Department of Energy. “Energy Department Announces New Investment in U.S. Small Modular Reactor Design and Commercialization.” News release. <http://energy.gov/articles/energy-department-announces-new-investment-us-small-modular-reactor-design-and> (accessed November 23, 2012).
- U.S. Department of the Navy. Center for Naval Analysis. *Feasibility of Nuclear Power on U.S. Military Installations*, by Marcus King, LaVar Huntzinger, and Thoi Nguyen. U.S. Department of Defense, March, 2011.
- U.S. Energy Information Administration. “Annual Energy Outlook 2012: Levelized Cost of New Generation Resources in the Annual Energy Outlook 2012.” http://www.eia.gov/forecasts/aeo/electricity_production (accessed February 20, 2013).
- U.S. Energy Information Administration. “Average Retail Price of Electricity to Ultimate Customers by End-Use Sector, 1999 through 2010 (cents per kilowatt hour).” Electric Power Annual 2010 Data Tables, Table 7.4. <http://www.eia.gov/electricity/annual/html/table7.4.cfm> (accessed December 29, 2012).
- U.S. Energy Information Administration. “Average Retail Price of Electricity to Ultimate Customers by End-Use Sector, by State, September 2012 and 2011.” http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_06_a (accessed November 25, 2012).

- U.S. Energy Information Administration. "Electric Power Annual 2010 Data Tables, Table 1.2 Existing Capacity by Energy Source, 2010 (Megawatts)." <http://www.eia.gov/electricity/annual/html/table1.2.cfm> (accessed December 14, 2012).
- U.S. Environmental Protection Agency. National Risk Management Research Laboratory, Office of Research and Development. *Environmental Technology Verification (EVT) Program Case Studies: Demonstrating Program Outcomes Volume II*. U.S. Environmental Protection Agency. Washington, DC, September 2006.
- U.S. Joint Chiefs of Staff. *2010 Joint Strategic Capabilities Plan*. Chairman of the Joint Chiefs of Staff Instruction 3110.01H Washington, DC: Joint Chiefs of Staff, June 10, 2011.
- Whitmore, Chris. "Nanosolar's Flexible Foil Technology Achieves 17.1% Aperture Efficiency in NREL Tests." http://www.pv-tech.org/news/nanosolars_flexible_foil_technology_achieves_17.1_aperture_efficiency_in_nr (accessed December 29, 2012).
- Zook, Matthew and Mark Graham. "Wal-Mart Nation: Mapping the Reach of a Retail Colossus," in *Wal-Mart World: The World's Biggest Corporation in the Global Economy*, 16. Edited by Stanley D. Brunn. New York: Taylor & Francis Group, 2006.

VITA

Most recently, he completed his Aviation Department Head tour at VAW-124 stationed at Norfolk, VA, from 2009-2012. LCDR Sagunsky was commissioned in 1998 from the U.S. Naval Academy. Following initial flight training, he reported to VAW-115 in Atsugi, Japan, where he served as the Ground Safety Officer, Personnel Officer, Line Division Officer, and Assistant Operations Officer from 2003-2006. He then reported for flight instructor duty at VAW-120 in Norfolk, VA, and served as the Aircraft Branch Officer, Avionics Division Officer, Assistant Training Officer, and Administrative Officer from 2006-2008. This was followed by one year at the U.S. Naval War College earning a Master of Arts in National Security and Strategic Studies.