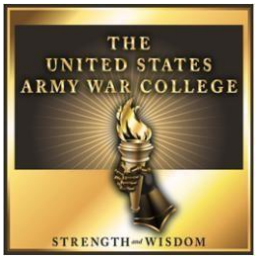
Strategy Research Project

Blackout! The National Guard's Response to a Cyberattack on the Grid

by

Lieutenant Colonel James P. Schreffler
United States Army

Under the Direction of:
Mr. Peter R. Hull



United States Army War College
Class of 2016

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-04-2016	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Blackout! The National Guard's Response to a Cyberattack on the Grid

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel James P. Schreffler
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Mr. Peter R. Hull

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
Please consider submitting to DTIC for worldwide availability? **YES:** ☐ **or NO:** X **(student check one)**
Project Adviser recommends DTIC submission? **YES:** ☐ **or NO:** ☐ **(PA check one)**

13. SUPPLEMENTARY NOTES
Word Count: 5,980

14. ABSTRACT

The United States power grid is a vital piece of the country's infrastructure. However, due to an increased reliance on computers, the system has become increasingly susceptible to a cyber attack. This paper provides an overview of the power grid and discusses its vulnerability to a cyber attack that would result in a catastrophic blackout. The National Response Framework is examined to include the role of the National Guard in a response to such an attack. The paper finds that the Guard focuses more on its wartime mission and is not structured or equipped to provide effective assistance to state governors during a catastrophic blackout. The author raises several proposals and further research questions to include the establishment of a National Guard pre-positioned stocks program as well as the establishment of separate home defense forces at the state level.

15. SUBJECT TERMS
DSCA, Dual Use Equipment, Power Grid

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(w/ area code)*
UU	UU	UU	UU	27	

Blackout! The National Guard's Response to a Cyberattack on the Grid

(5,980 words)

Abstract

The United States power grid is a vital piece of the country's infrastructure. However, due to an increased reliance on computers, the system has become increasingly susceptible to a cyber attack. This paper provides an overview of the power grid and discusses its vulnerability to a cyber attack that would result in a catastrophic blackout. The National Response Framework is examined to include the role of the National Guard in a response to such an attack. The paper finds that the Guard focuses more on its wartime mission and is not structured or equipped to provide effective assistance to state governors during a catastrophic blackout. The author raises several proposals and further research questions to include the establishment of a National Guard pre-positioned stocks program as well as the establishment of separate home defense forces at the state level.

Blackout! The National Guard's Response to a Cyberattack on the Grid

Since the birth of this country, citizens of the United States have faced multiple threats to their safety and well-being. These threats include natural causes, such as earthquakes and hurricanes, as well as the hostile acts of enemies. A new, but increasingly possible threat has emerged in recent years in the form of a computer attack on the nation's power grid. To meet this intentional threat, as well as others from natural causes, the U.S. Government has constructed a response framework made up of multiple departments and agencies at the federal level. While these federal agencies possess vast resources, state and local agencies play an important role as well and must integrate into any national response. One such agency that is key to any national emergency is the National Guard. Although the National Guard is an essential element of the response framework, it remains more focused on wartime tasks than supporting the state Governors in a response to a catastrophic blackout. The National Guard must be just as prepared for such a blackout as they currently are to support the U.S. in overseas conflicts

Cyber Warfare and the Power Grid

United States citizens and industry alike often take for granted the benefits and importance of the electric power grid despite the increased reliance they place upon it to conduct daily business. However, when those benefits and comforts are interrupted, citizens realize the importance of the electric grid in sustaining both the quality and security of life to which the they are accustomed. While the interruption of electric service, usually due to natural causes, is a routine event throughout the power grid structure, these interruptions are usually localized and temporary in nature, affecting only a small portion of the system. Service providers and the public alike have become

quite adept at handling these service interruptions, viewing them more as a nuisance than anything else, because service is usually restored in a matter of hours. Although temporary outages due to natural causes are routine, the likelihood of a hostile interruption of power service on a large scale is becoming more of a possibility.

While technology has drastically improved the quality of life in the United States, it has also created a society that is increasingly reliant on technology and automation to provide for daily needs. This increased reliance on computer technology to provide services makes the computerized systems of both private and public industry alike more susceptible to unauthorized access by hackers. Countless corporate computer security breaches, such as the Target credit card breach, show the vulnerability of computer networks to such an attack.[1] The power grid infrastructure is one element of industry that is subject to unauthorized access due to its dependence on computer automation and the internet for operations.

The vulnerability of the power grid system to a cyber-attack by a hostile state is of great concern to many involved in critical infrastructure administration and security. Director of National Intelligence James Clapper demonstrated this in his February 2015 threat assessment report to the U.S. Senate Armed Services Committee, which states, “Computer security studies assert that unspecified Russian cyber actors are developing means to access industrial control systems (ICS) remotely. These systems manage critical infrastructure such as electrical power grids, urban mass transit systems, air traffic control, and oil distribution networks.”[2] It appears that this assessment was extremely accurate, as less than a year later on December 23, 2015, Ukraine experienced a hostile cyber attack on their power grid. The attack intentionally disrupted

power service to over 700,000 homes in Western Ukraine for several hours. Investigators believe that the Russian state sponsored hacking group, Sandworm conducted the attack by implanting the Black Energy malware into Ukraine's power grid computer system.[3] Not only is this attack significant in that it is the first successful cyber attack resulting in an interruption of power service, but authorities also discovered the same Black Energy malware in the United States power grid system.[4] According to the Department of Homeland Security, in the May/June 2015 issue of their Industrial Control Systems Cyber Emergency Response Team (ICS – CERT) newsletter, a publication provided to the private power supply industry, the Black Energy malware was also inserted into the U.S. power grid in 2015 through suppliers who had their systems connected to the internet.[5] In order to gain a better understanding of the power grid vulnerability, one should have a basic understanding of its construction and operation.

Understanding the Grid

The United States power grid actually consists of three separate grids divided into geographic sectors of the country. The largest grid covers the country from the eastern seaboard to a point just west of the halfway point and extends from the northern border south to a point within the state of Texas. The western grid then picks up from that point and extends to the western seaboard. The third grid is limited to almost the entire state of Texas (see Figure 1).[6] The map in Figure 1 illustrates the extent to which a successful attack on just one section of the grid will affect the public. With each section of the grid covering thousands of square miles and providing power to millions of people, government authorities will require the assistance of agencies at all levels, to include the National Guard, in dealing with the response. Considering the enormity and importance of the grid, one would think that the U.S. Government administers it.

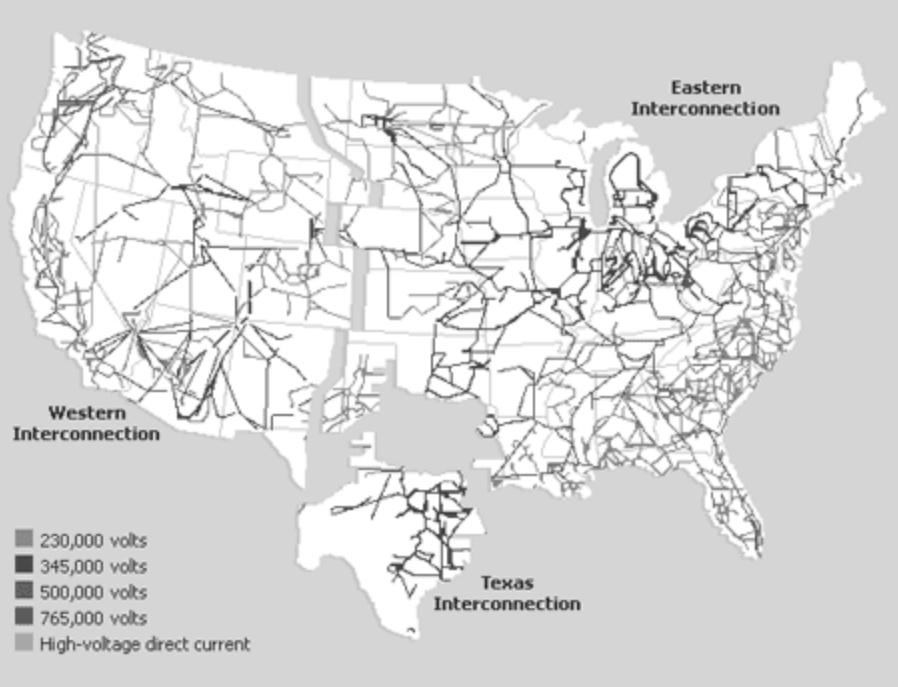


Figure 1: Map of United States Power Grid Structure[7]

Contrary to popular belief, the United States Government does not own, or operate the U.S. power grid. Although it is a key element of the country's critical infrastructure, and overseen by the government, the grid is a system made up largely of private enterprise. Numerous primary power generation stations, owned by various electric companies throughout the system, provide power for the entire grid. Thousands of miles of high voltage transmission lines transport this power throughout the grid to private enterprise sub stations that distribute the electricity via lines to the end user. During this process, the electricity passes through several Large Power Transformers (LPTs) to step up or step down voltage as required.[8] These components in themselves may be vulnerable to an isolated physical attack, but their collective dependence on computer control networks increases the vulnerability of the entire system.

Vulnerability of the Grid

While there is some risk to the physical components of the grid from nature or sabotage, the primary vulnerability lies in the system's reliance upon computer automation and the internet for proper synchronization and distribution of power. As the Department of Homeland Security points out in its bulletin to industry providers, providers connected to the internet, are susceptible to unauthorized access.[9] Ted Koppel's book, *Lights Out* regarding the topic of a cyber attack on the power grid has received much attention in the media recently and points out particular vulnerabilities in the power grid structure.

In his 2015 book, Koppel identifies key elements within the power grid structure that are particularly vulnerable to manipulation by hostile actors. One of the vulnerable areas is the group of systems used to coordinate, link and control operations throughout the grid. These supervisory control and data acquisition systems (SCADA) are particularly vulnerable because of a lack of design diversity due to their manufacture by a small number of companies.[10] As Koppel learned in an interview with Richard Clarke, the chairman of a cyber security risk management firm, "'if you go into a big, modern, power station in Shanghai, or a big, modern, power station in California, you're going to find the same SCADA software.'"[11] This is particularly alarming considering the success of the infiltration and attack on the modern power system in Ukraine, which presumably uses this common SCADA software. While the control operations in the power grid are very complex, "if someone was knowledgeable about the functions of a SCADA system and succeeded in hacking into it, that individual could engineer 'a series of events that seem totally unrelated' but which could, 'turn the lights out very quickly over large

areas.'"[12] Another particularly vulnerable area in the system are the LPTs used to modify electricity voltage in the transmission process.

As noted previously, the electric power grid relies on large LPTs for the safe delivery of electricity at various points throughout the system. The importance of these LPTs to the distribution of power is evident in the fact that there are thousands of them in the system. They are so numerous that even the Department of Energy does not know how many are in use throughout the grid, but believes there "'could be in the range of tens of thousands'" of them.[13] With the system relying so heavily on the use of LPTs, one would believe that these items are mass produced and easily replaceable. This however, is not the case. According to the same Department of Energy report, the LPTs are manufactured to unique specifications and weigh as much as 410 tons. Because of their enormous size, the LPTs require specialized transportation assets to move them, of which there are a limited number. Additionally, they require a manufacturing "lead time of between five and 16 months; however, the lead time can extend beyond 20 months if there are any supply disruptions or delays with the supplies, raw materials, or key parts."[14] Essentially, the U.S. power grid relies heavily on a piece of equipment that if rendered ineffective, is neither abundantly available nor quickly replaced. "Failure of a single unit could result in temporary service interruption and considerable revenue loss. . . . Should several of these units fail catastrophically, it will be challenging to replace them."[15] Additionally, should a sinister actor gain control of the power grid through the internet and manipulate elements of the system, such as the SCADAs or LPTs, in order to cause damage, and responding agencies, to include the

National Guard are not equipped to fill these capability gaps, the results could be catastrophic.

Effects of an Attack

Utility companies have become very proficient in restoring power during temporary outages due to natural causes and their effects on the physical elements of the grid. However, if a hostile actor, with knowledge of the power grid, gains access to vital components through the computer network and causes them to malfunction, the resulting effects would likely last for an extended period of time. Koppel reinforces this idea when describing the difference in the effects of a natural disaster and a cyber attack:

> For one thing, the affected area could be much greater. Even a partial blackout of a grid could lead half a dozen or more states without electricity. Also, unless one credits the Old Testament - style intervention of an angry deity, storms do not deliberately target a system's critical weaknesses. Cyber-attacks do, and if we assume that the attackers are predisposed to inflict maximum damage, they will try to conceal what they are doing.[16]

The long lasting effects of such an attack on our society and way of life are difficult to comprehend without further study.

Many U.S. citizens do not think a successful cyber attack on the power grid is possible. As a result, many are not aware of the seriousness of the long-term effects such an attack would have. Koppel provides a vivid and stark reality of the effects a long term, wide scale power outage would have on society and provides insight on the challenges facing response agencies:

> Extended periods of darkness, longer and more profound than anyone now living in one of America's great cities has ever known.
> As power shuts down there is darkness and the sudden loss of electrical conveniences. As batteries lose power there is the more gradual failure of cellphones, portable radios, and flashlights.

> Emergency generators provide pockets of light and power, but there is little running water anywhere . . . . [T]aps go dry; toilets no longer flush. Emergency supplies of bottled water are too scarce to use for anything but drinking, and there is nowhere to replenish the supply. Disposal of human waste becomes a critical issue within days.
> Supermarket and pharmacy shelves are empty in a matter of hours. . . . There is no immediate resupply, and people become desperate.
> For the first couple of days, emergency personnel are overwhelmingly engaged in rescuing people trapped in elevators. . . . Home care patients reliant on ventilators and other medical machines are already dying. . . . Almost everyone needs some kind of assistance, and no one has adequate information.
> The city has flooded the streets with police to preserve calm, to maintain order, . . . People are less concerned with what exactly happened than with how long it will take to restore power. . . .
> There is a growing awareness that this power outage extends far beyond any particular city and its suburbs. It may extend over several states. Tens of millions of people appear affected. Fuel is beginning to run out. . . . [G]as stations without backup generators are unable to operate their pumps. Those with generators are running out of fuel and shutting down. . . . The majority who believed that power outages are limited in duration, that help always arrives from beyond the edge of darkness, is undergoing a crisis of conviction.[17]

While the above example may seem exaggerated to some, it is absolutely possible that the scenario described could result from a sophisticated cyber attack. Obviously, such an event would require a massive response to provide for the security and well-being of the citizens that would involve all levels of government.

All Hazards Response

On March 11, 2011, President Barak Obama issued Presidential Policy Directive (PPD) 8 with the intent of increasing U.S. preparedness for a catastrophic event. While PPD 8 focuses on the national level, it directs agencies to develop operational plans that facilitate coordination among all levels of government, from municipal to federal.[18] To meet the goals laid out in PPD 8, the Federal Emergency Management Agency (FEMA) developed the National Response Framework (NRF). This framework covers all aspects of preparedness, from prevention through recovery operations, and is a “guide

to how the nation responds to all types of disasters and emergencies."[19] Although written and published at the national level, the NRF stresses the importance of preparedness at the lowest level, beginning with the individual or family, and continuing up the continuum through local and state governments before culminating in a federal response. Considering the multitude of incidents that could occur, the NRF utilizes data from the Strategic National Risk Assessment (SNRA) to focus on the most prominent risks to the country. The NRF then uses these risks to develop NRF Incident Annexes and the Federal Interagency Operations Plan (FIOP).[20] Additionally, the NRF identifies 14 core capabilities required of governments during a crisis and the associated emergency support functions (ESF) necessary to meet them. The framework then assigns a lead agency to each ESF to coordinate efforts in that particular functional area.[21]

The NRF Incident Annexes tailor ESF responses to specific contingencies and assign duties to the agencies involved. The contingency situations identified in the latest NRF Incident Annex consist of the following types of incidents: Biological, Catastrophic, Cyber, Food and Agriculture, Mass Evacuation, Nuclear/Radiological, and Terrorism.[22] A review of the annexes reveals that none of them specifically address the response to an attack on a power grid with a long-term interruption. While the Cyber Attack Incident Response Annex addresses an interruption of critical infrastructure, it focuses solely on the computer aspect of the incident and does not address any of the consequences of such an incident and the effects on the populace.[23] The Catastrophic Incident Annex somewhat encompasses the results of an attack on a power grid in its definition of a catastrophic event as "any natural or manmade incident, including terrorism, that results

in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions."[24] However, as with the rest of the NRF, the annexes focus on the response of Federal agencies, with little guidance given to state or local governments.

Although the NRF is meant for use by all levels of government, the focus of the framework is on the Federal level. The guidance given to state and local levels is fairly general in nature and consists of statements such as, "State governments supplement local efforts before, during, and after incidents by applying in-state resources first. If a state anticipates that its resources may be exceeded, the governor may request assistance from other states or the Federal Government."[25] While the NRF does not clearly discuss state resources, and no ESFs are assigned to state agencies, a key asset available to the governor of any state for use in responding to a power grid interruption is the National Guard.

National Guard Background

The Army National Guard is a critical element of the U.S. Armed Services. Together, with the Army Reserve, the two forces make up the Reserve Component of the total Army force. However, unlike the Army Reserve, the National Guard has an important state mission in addition to its Federal mission as an operational reserve to the Army. Since its inception in 1636, the Army National Guard has played a key role in the defense and well-being of the local community.[26] Made up of local citizens, the unit would muster under local direction when danger threatened the community. Once the threat to community safety was over, the members would disband and return to their homes. Throughout history a variety of significant historical documents, including the

U.S. Constitution, have reaffirmed the concept of local control of the militia, which eventually evolved into the National Guard.

The value and role of the National Guard as part of the Total Army Force is evident in numerous pieces of historical legislation. The U.S. Constitution clearly illustrated the value of the militia to national security. Article 1, Section 8, states that the President may call for a mobilization of the militia to support the Union in times of crisis but otherwise to "reserving to the States respectively, the Appointment of the Officers, and the Authority of training the Militia according to the discipline prescribed by Congress."[27] Shortly after the writing of the Constitution, the Militia Act of 1792 established the National Guard as the official reserve of the U.S. Army, which allowed for an increase of funding and equipment for the force.[28] Several legislative acts, including the National Defense Act of 1916, further solidified the National Guard's role as the reserve of the Federal Army.

Throughout much of the twentieth century, the National Guard suffered from somewhat of an identity crisis. While the Governors wanted to maintain control of their respective units to meet local security threats, the active Army saw the National Guard as a way to increase their combat capability while not having to maintain a large standing army. As a result, federal funding, equipping and training guidance seemed to focus solely on the wartime mission of the units. State legislatures however, perceived the threat to state security to be real enough that the National Defense Act of 1916 allowed states to raise additional reserve forces for state duty when their National Guard units deployed for Federal service. Congress endorsed this concern by passing The Home Defense Act of 1917, authorizing sates to form home defense forces. These

forces were separate from the National Guard, equipped by the Federal Government, and designed to act in civil defense roles.[29] It was not until the mid-twentieth century that the home defense mission began to shift back to the National Guard.

Throughout the mid twentieth century during the turbulent times of World War II and the Korean War, the need for the additional home defense units remained high as the National Guard was heavily involved in the war efforts. Following the Korean War, and the slowed pace of deployments, more National Guard units were able to remain at home in their states. Due to this fact, coupled with the Army's increased reliance on the newest member of the Total Force, the Army Reserve, the need for the extra expense of the home defense units began to lessen.[30] The National Guard began to focus once again on the added civil defense responsibility but found that years of war, coupled with Federal funding and equipping resulted in their units being better suited for combat than assistance to civil authorities. The Cold War brought about a renewed concern for security at the local level and revitalized the call for additional state defense forces. Under the direction of the Department of Defense, the National Guard Bureau set forth regulations in 1987 governing the formation, equipping, training and control of additional state forces. Under the regulation, the forces would fall under the sole control of the Governor whereas the National Guard Bureau would provide funding and training oversight. However, as Dr. Kent Sieg points out in his report, "America's State Defense Forces: An Historical Component of National Defense," this system was not successful.

> [A]s the years went by the National Guard failed to oversee, train, and utilize the state guards. Constraints in this complex relationship included the priorities of the National Guard's federal versus state missions, the lack of discipline and command and control within the state defense forces themselves, funding limitations, and legal restrictions. The National Guard simply did not want the state defense forces.[31]

Although there are still remnants of the additional state defense forces in existence today, the responsibility of civil defense fell back on the National Guard when it declared, “it was fully capable of meeting its state obligations.”[32] To assist in its role as a primary tool for state governors for domestic operations, there are National Guard units spread throughout 54 states and territories in approximately 2,600 communities.[33] Not only does this unit arrangement provide a military link to the community, it also offers a quicker response during state emergencies.

Dual Missions of the National Guard

In order to better understand the National Guard state mission a review of the terms “Homeland Defense” and Defense Support to Civilian Authorities (DSCA) is necessary. “Homeland Defense” is defined in Title 32 of the United States Code as, “an activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or aggression against the United States.”[34] DoD Directive 3025.18 defines DSCA as,

> Support provided by U.S. Federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. Also known as civil support.[35]

The distinction of the two terms is important in that Homeland Defense focuses on the protection aspect, while DSCA encompasses assistance to civilian authorities in response and recovery operations during natural or manmade disaster and other emergencies. While both the Active and Reserve Components of the Army can

participate in these two missions, legal restrictions often make it more convenient for the National Guard to fulfill the role of Homeland Defense and DSCA.

A primary consideration in the employment of military forces in homeland operations is the Posse Comitatus Act (PCA). The PCA prohibits the participation of federalized military members in certain activities when in domestic support of civilian law enforcement agencies (DSCLEA). These restrictions include vehicle interdiction, search and seizure, arrests and apprehensions, using force, and security functions, to include crowd control.[36] Although, DSCA and DSCLEA operations are considered separate, a review of the definition of DSCA leads one to believe that units mobilized in support of DSCA operations may find themselves actually conducting DSCLEA activities and thus subject to PCA restrictions. As stated, PCA restrictions only apply to federalized forces and not to the National Guard when in their state status. It is then clear why the National Guard

> ha[s] primary responsibility to support State and local Government agencies for disaster responses and in domestic emergencies, including in response to civil disturbances; such activities would be directed by, and under the command and control of, the Governor, in accordance with State or territorial law and in accordance with Federal law.[37]

Despite its designation as the primary military agency for DSCA operations, the National Guard's structure may better suit its role as an operational reserve to the Army.

Although, communities with a National Guard unit benefit from their personnel manpower, the unit may not be equipped properly for emergency response functions. The Army National Guard currently consists of eight divisions,

> 126 operational brigades and groups; including 28 Brigade Combat Teams (Infantry, Armor, and Stryker), 48 multi-functional support brigades (including combat aviation, surveillance and sustainment brigades), 48 functional support brigades and groups (including military police, engineer and regional support) and 2 Special Forces Groups.[38]

In order to accomplish both of their missions, it is essential that these units be properly equipped to do so.

Equipping the Guard for Blackout Response

Adequate equipping of the National Guard has long been a concern for the force as historically they lagged behind in funding as well as modernization. However, since September 11, 2001, due to an increased role as an operational reserve, the equipping situation to meet their combat roles has improved drastically. “The ARNG of 2015 is manned, trained, equipped, and experienced at historically high levels. . . . In 2011, ARNG Equipment On-hand (EOH) was at 77 percent. At the end of FY 2014, total EOH was up to 93 percent.”[39] Once again, the focus is on equipping these units to fulfill their wartime missions, not for specific DSCA missions. However, the National Guard categorizes some elements of the EOH as critical dual use (CDU) equipment. These items are pieces of equipment that the Guard considers necessary to meet the unit’s wartime mission and may also be useful during DSCA missions. The goal of the Guard is to maintain at least an 80% EOH rate for CDU equipment.[40]

While the National Guard has enjoyed an increase in total EOH levels across the board, some of their CDU items, which will be essential in a power grid outage, fall below their 80% on-hand rate. Table 1 displays some of the CDU designated equipment levels. Not only are some of the EOH levels of CDU equipment in Table 1 very low, the table does not take into account the readiness status or availability of the equipment that is on hand. Additionally, the Guard lists 57 line items worth of generator equipment as CDU, which are not contained in Table 1. Of these 57 items, the EOH value will decrease by the end of Fiscal Year 2018, further reducing power generation capacity.[41]

Table 1: CDU Equipment Percent Fill[42]

CDU Equipment	% On Hand
UH-60 Blackhawk (Modernization)	76
Aviation Ground Support Equipment (54 line items)	65
Chemical Biological Protective Shelter (CBPS)	3
2,000 gal. Water Tank-Rack (HIPPO)	39
Assault Kitchen	42
HMMWV Ground Ambulance	100
Tank Fabric Collapsible: Water 3000 gal.*	3**
Water Storage/Distribution Set: 40K-gpd	16**
* Not officially designated as CDU ** Based on projected on-hand vs. required at end of FY '18	

Although a review of EOH numbers reveals an impressive array of equipment, state governors only have access to the equipment assigned to units in that state. The type of unit often limits the capability and capacity to respond to a domestic emergency, such as a large-scale power interruption. For example, some units, such as engineers have obvious combat functions, skills and equipment that are also useful in a state emergency response. Others, such as an Armored Brigade Combat Team (ABCT), are not so easily adapted to this task. While the main battle tanks and tracked armored personnel carriers definitely enhance the combat capability of the Army, they are of little use to the state governor during disaster response involving a power grid outage.

As identified by their CDU designation, it is likely that wheeled vehicles, generators, ambulances, and water distribution systems will be in high demand for an

power grid emergency response situation. Table 2 below illustrates the equipment organic to an ABCT that falls into the categories discussed above.

Table 2: ABCT Organic Equipment[43]

Equipment	Number*
Generator Sets	175
HMMWV**	388
Trucks (Other)	219
Ambulance (Wheeled)	9
Water Tanks	45
* Numbers are from the Table of Equipment (TOE) and may not reflect the Modified TOE (MTOE). ** High Mobility Multipurpose Wheeled Vehicle	

Although the equipment contained in Table 2 may seem adequate for a response, it is important to remember that the equipment is distributed among approximately 38 units throughout the brigade, which are not all collocated.[44] It is common in the National Guard to have subordinate units of a major command spread out over the entire state and in some instances, over multiple states. Furthermore, the availability of unit equipment is dependent on qualified personnel available to operate it. If the unit deploys in support of combat operations or another domestic operation, its personnel and/or equipment may not be available for use. Additionally, it is not realistic to believe that all the equipment listed will be fully mission capable (FMC) when needed. An overview of generator status in a National Guard Combat Aviation Brigade revealed that 15% of their assigned generators and approximately 17% of their trucks were not available for use at the time of their status report due to either scheduled maintenance or

unserviceable conditions.[45] Because of standardized maintenance schedules and common usage practices throughout the Guard, one can assume that these non-availability rates are somewhat consistent across the force. Of the equipment available for use, the majority of it would likely be necessary to support internal unit operations during an emergency, further limiting what is available to civil authorities.

Outside of some limited, specialized units, the majority of National Guard units are sourced with equipment necessary to complete their wartime mission. Although some of their equipment may receive CDU designation, generally, units do not receive extra equipment to use for DSCA missions. As a result, during the scenario of a long term, wide scale, power grid interruption where generators will be in high demand, the unit will use the majority of them to conduct internal operations such as sustainment and command and control functions. A National Guard aviation unit confirmed that during an emergency involving a power outage in their area, it was planning to use only two of its 25 assigned generators for assisting civil authorities. The unit needed the remaining generators to support their own operations and further pointed out that the generators were not able to provide power to some civilian buildings due to wiring incompatibility.[46] Despite the issues highlighted concerning the capability of the National Guard to assist civil authorities during a severe power grid interruption, there are several possibilities available to assist the Guard in meeting this need.

Conclusion

The increasing likelihood of an attack on the U.S. power grid poses serious concerns for civil authorities. To assist in responding to such a large-scale emergency, FEMA has developed the NRF that provides some guidance for all levels of government, with an emphasis on the Federal response. This framework highlights the

National Guard as a key element available to the governors during such a large-scale emergency. However, although the Guard is a large organization, and spread out across the entire country, it is more focused and equipped for their wartime mission. Furthermore, unit and equipment availability during a large-scale power outage may be limited due to deployments and equipment serviceability status. Even if available, these units will be dealing with the same conditions that the public and civil authorities are and will need to use much of their equipment to support their own internal operations. To assist the force in equipment shortage and availability for combat the Active Component has established extra, pre-positioned equipment around the world.

The [Army Prepositioned Stocks] APS program is critical to the ability of the Army to complete its mission. The APS "consists of prepositioned unit sets of equipment, operational project stocks, Army War Reserve Sustainment Stocks and War Reserve Stocks for Allies."[47] These sets of equipment, strategically placed around the world allow the Army to respond to a threat to national security quickly through an increased force projection capability. This same concept, if applied by the National Guard, would increase its capability to respond to large-scale power interruptions as well as other emergencies. Equipment sets with extra generators, wheeled vehicles, water purification and distribution systems should be strategically placed in each state or, at a minimum, in each of the ten FEMA regions. This system would allow the governor to better utilize the units of the states by allowing them to use their own equipment to support their internal needs while drawing from the emergency equipment set to support the mission. Although an APS system for the National Guard will enhance its ability to

respond to state missions, decreased funding levels may inhibit the Guard from meeting both elements of its dual mission equally well.

Due to combat operational tempo since September 11, 2001, the National Guard has enjoyed increased funding and equipping levels. However, with the decrease of operations in Afghanistan and Iraq, these levels will not remain the same. Already, under the current fiscal situation the total Army is facing personnel cuts to levels lower than before 2001.[48] Lower equipping levels will accompany these force cuts and make it more difficult for the National Guard to complete both its DSCA and combat roles effectively. Because of these same fiscal constraints, the active Army has no choice but to rely more heavily on the National Guard as an operational, combat reserve.

The increased reliance on the National Guard to round out active Army combat capability may require the Guard take a hard look at its priorities. Should it focus on equipping and training to serve in combat, or focus on structure, equipping, and training that better supports the state governors? The Guard has proven itself capable in combat through countless deployments since 2001. It may be time for the Guard to pick a role and commit fully to it in terms of structure, personnel and equipment. Should the Guard consider a restructure to the days that included a separate and distinct civil defense force under the oversight of the Guard? Some such as Sieg say it is.

> The state guards would not interfere with federal or National Guard missions but would instead complement them. 'The State Guard/Home Guard company costs virtually nothing in new budget appropriation,' former longtime State Guard Association of the United States (SGAUS) President Paul McHenry noted back in 1998. 'It supports but does not lead the civil government. It fills in behind police, the emergency manager, and any other agency within the purview of its function. The home guard company has support as its function – support of those with expertise. Home guard has nothing to do with warrior classes of the Armed Forces.[49]

This option, while a dramatic shift from the current situation, is feasible and begs further consideration. This force structure option seems to offer more of a benefit to state governors and allows the Guard to continue to focus on its role as a combat reserve. What drives National Guard force structure and how much say the governors have in the process is also worthy of further study. What seems to be certain, under current structure and equipping the National Guard will be plunged into darkness with the rest of the civilian population during the blackout.

Endnotes

[1] Robin Sidel, Danny Yadron, and Sara Germano, "Target Hit by Credit-Card Breach," *The Wall Street Journal Online*, December 19, 2013, http://www.wsj.com/articles/SB10001424052702304773104579266743230242538 (accessed January 4, 2016).

[2] James R. Clapper, *Worldwide Threat Assessment of the U.S. Intelligence Community: Statement for the Record to the Senate Armed Services Committee* (Washington, DC: Director of National Intelligence, February 26, 2015), 3, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed December 8, 2015).

[3] Nilufer Tuptuk and Stephen Hailes, "The Cyberattack on Ukraine's Power Grid is a Warning of What's to Come," January 13, 2016, http://phys.org/news/2016-01-cyberattack-ukraine-power-grid.html (accessed January 13, 2016).

[4] Shane Harris, "CIA Eyes Russian Hackers in Blackout Attack," January 6, 2016, http://www.thedailybeast.com/articles/2016/01/06/exclusive-cia-eyes-russian-hackers-in-blackout-attack.html (accessed January 6, 2016).

[5] U.S. Department of Homeland Security, "If You're Connected, You're Likely Infected!" *ICS-CERT Monitor,* May/June, 2015, 4, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf (accessed December 16, 2015).

[6] U.S. Department of Energy, "Top 9 Things You Didn't Know About America's Power Grid," November 20, 2014, http://energy.gov/articles/top-9-things-you-didnt-know-about-americas-power-grid (accessed January 3, 2016).

[7] Ibid.

[8] Ibid.

[9] U.S. Department of Homeland Security, "You're Connected, You're Likely Infected!" 4.

[10] Ted Koppel, *Lights Out, A Cyberattack, A Nation Unprepared, Surviving the Aftermath* (New York: Crown Publishing Group, 2015), 38.

[11] Ibid., 39.

[12] Ibid.

[13] U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid* (Washington, DC: U.S. Department of Energy, June 2012), 20, http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf (accessed January 6, 2016).

[14] Ibid., 31.

[15] Ibid., 1.

[16] Koppel, *Lights Out, A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, 114.

[17] Ibid., 3-5.

[18] Barak Obama, "Presidential Policy Directive 8/PPD 8: National Preparedness," March 11, 2011, http://www.dhs.gov/presidential-policy-directive-8-national-preparedness (accessed December 13, 2015).

[19] U.S. Department of Homeland Security, *National Response Framework,* 2nd ed. (Washington, DC: U.S. Department of Homeland Security, May 2013), 1, https://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf (accessed December 7, 2015).

[20] Ibid., 7.

[21] Ibid., 20,31.

[22] Federal Emergency Management Agency, "National Preparedness Research Library," last modified December 23, 2015, http://www.fema.gov/national-preparedness-resource-library (accessed February 7, 2016).

[23] Federal Emergency Management Agency, *Cyber Incident Annex* (Washington, DC: U.S. Department of Homeland Security, December 2004), http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf (accessed February 12, 2016).

[24] Federal Emergency Management Agency, *Catastrophic Incident Annex* (Washington, DC: U.S. Department of Homeland Security, November 2008), http://www.fema.gov/media-library-data/20130726-1825-25045-3106/catastrophic_incident_annex_2008.pdf (accessed February 12, 2016).

[25] U.S. Department of Homeland Security, *National Response Framework,* 3.

[26] National Guard, "About the Army National Guard," http://www.nationalguard.mil/AbouttheGuard/ArmyNationalGuard.aspx (accessed February 13, 2016).

[27] U.S. Constitution, art. 1, sec. 8, cl. 16.

[28] William M. Donnelly, "The Root Reforms and the National Guard," May 3, 2001, http://www.history.army.mil/documents/1901/Root-NG.htm (accessed February 14, 2016).

[29] Kent G. Sieg, "America's State Defense Forces: An Historical Component of National Defense," 2005, linked from the *Defense Technical Information Center Home Page* at "Technical Reports," http://www.dtic.mil/dtic/tr/fulltext/u2/a497658.pdf (accessed February 15, 2016), 4.

[30] Ibid., 5.

[31] Ibid.

[32] Ibid.

[33] National Guard Bureau, *2015 National Guard Posture Statement, Trusted at Home, Proven Abroad*, *Fiscal Year 2015* (Washington DC: U.S. Department of Defense, 2014), 15.

[34] U.S. Code, Title 32, Chapter 9, "Section 901 Definitions," Amended October 28, 2004, http://uscode.house.gov/view.xhtml?hl=false&edition=prelim&path=&req=granuleid%3AUSC-2014-title32-section901&fq=&num=0 (accessed February 15, 2016).

[35] U.S. Department of Defense, *Defense Support of Civil Authorities (DSCA)*, Directive No. 3025.18 (Washington, DC: U.S. Department of Defense, December 29, 2010), 16, http://www.dtic.mil/whs/directives/corres/pdf/302518p.pdf (accessed February 15, 2016).

[36] U.S. Department of Defense, *Defense Support of Civilian Law Enforcement Agencies (DSCLEA)*, Directive No. 3025.21 (Washington, DC: U.S. Department of Defense, February 27, 2013), 17.

[37] Ibid., 27.

[38] National Guard Bureau, *2015 National Guard Posture Statement, Trusted at Home, Proven Abroad*, 15.

[39] U.S. Department of Defense, *National Guard and Reserve Equipment Report for Fiscal Year 2016*, ed. Matthew W. Lucas (Washington, DC: U.S. Department of Defense, March 2015), 1-8.

[40] Ibid., 1-9.

[41] Ibid., ARNG 1-2 – 1-3.

[42] Ibid., 2-21 – 2-24, ARNG 1-2 – 1-3.

[43] Maneuver Center of Excellence Organizational Development Branch, *MCoE Supplemental Manual 3-90* (Ft. Benning, GA: Maneuver Center of Excellence, September 2012), 74-142, http://www.globalsecurity.org/military/library/policy/army/other/msm3-90_2012.pdf (accessed February 16, 2016).

[44] Ibid., 74.

[45] Missouri National Guard, LOGSTAT Report, July 20, 2015, unpublished.

[46] MAJ Paul Howerton, U.S. Army, Training Officer/Asst. S-3, 35th Combat Aviation Brigade, MOARNG, telephone interview by author, February 16, 2016.

[47] Association of the United States Army, "Army Prepositioned Stocks: Indispensable to America's Global Force-projection Capability," December 2008, 2, http://www.ausa.org/publications/torchbearercampaign/torchbearerissuepapers/documents/tb-ip_120308.pdf (accessed February 20, 2016).

[48] John M. McHugh and Raymond T. Odierno, *A Statement on the Posture of the United States Army 2015*, Posture Statement presented to the 114th Cong., 1st sess. (Washington, DC: U.S. Department of the Army, 2015), 16.

[49] Sieg, "America's State Defense Forces: An Historical Component of National Defense," 6.