National Security and Assured U.S. Electrical Power

CNA Military Advisory Board

November 2015

CNA
ANALYSIS & SOLUTIONS

Unlimited Distribution

Recommended citation:
CNA Military Advisory Board, *National Security and Assured U.S. Electrical Power*
(Arlington, VA: CNA, 2015)

CNA is a not-for-profit company which serves the public interest by providing in-depth analysis and results-oriented solutions to help government leaders choose the best course of action in setting policy and managing operations.

Approved for Unlimited Distribution

Cheryl B. Rosenblum
Executive Director, CNA Military Advisory Board

This report was developed with the support of the Energy Foundation.

The CNA Military Advisory Board

This document presents the wide-ranging views of an advisory group of retired flag and general officers from the Army, Navy, Air Force, and Marine Corps on the subject of national security and assured U.S. electrical power. Since 2006, this advisory group, referred to as CNA's Military Advisory Board (MAB), has examined the linkages between climate, energy, and national security, and has brought its vast operational, tactical, and strategic experience and perspective to domestic and international discussions. Past MAB reports include *National Security and the Threat of Climate Change*, *Powering America's Defense: Energy and the Risks to National Security, Ensuring America's Freedom of Movement: A National Security Imperative to Reduce U.S. Oil Dependence*, and the CNA MAB's most recent work, *National Security and the Accelerating Risks of Climate Change.*

More information about the CNA MAB, including an archive of all past reports, can be found on the CNA MAB's website, www.cna.org/mab.

General Ron Keys, USAF (Ret.)
CNA MAB Chairman
Former Commander, Air Combat Command

Brigadier General Gerald E. Galloway Jr., USA (Ret.), CNA MAB Vice Chairman
Former Dean at the United States Military Academy and former Dean at the Industrial College of the Armed Forces, National Defense University

Vice Admiral Lee Gunn, USN (Ret.)
CNA MAB Vice Chairman
Former Inspector General of the Department of the Navy

Admiral Frank "Skip" Bowman, USN (Ret.)
Former Director of Naval Nuclear Propulsion Program and former Chief of Naval Personnel

Lieutenant General Ken Eickmann, USAF (Ret.)
Former Commander, U.S. Air Force Aeronautical Systems Center

Lieutenant General Larry Farrell, USAF (Ret.)
Former Deputy Chief of Staff for Plans and Programs, Headquarters, U.S. Air Force

General Don Hoffman, USAF (Ret.)
Former Commander, U.S. Air Force Materiel Command

General Paul Kern, USA (Ret.)
Former Commanding General, Army Materiel Command

Vice Admiral Ann Rondeau, USN (Ret.)
Former President, National Defense University and Former Deputy Commander, U.S. Transportation Command

Lieutenant General Keith Stalder, USMC (Ret.)
Former Commanding General, U.S. Marine Corps Forces, Pacific

Rear Admiral David Titley, USN (Ret.)
Former Oceanographer of the Navy

General Charles "Chuck" Wald, USAF (Ret.)
Former Deputy Commander U.S. European Command

Lieutenant General Richard Zilmer, USMC (Ret.)
Former Commandant for Manpower and Reserve Affairs and Former Commanding General of Multi-National Force–West in Al Anbar Province, Iraq

MAB Executive Director:
Ms. Cheryl B. Rosenblum
Executive Director, CNA Military Advisory Board

CNA Team
Dr. Leo Goff, *Program Manager, Writer*
Dr. Mary "Kate" Fisher, *Lead Writer*

National Security and Assured U.S. Electrical Power

To the reader:

Reliable electricity underpins every facet of American lives. Without it, our homes, our businesses, and our national security engine would grind to a halt—especially when so much of this power is becoming "smart" and integrated. Yet the nation's electrical generation and distribution infrastructure, commonly referred to as "the grid," is showing its age and vulnerability—no wonder, since the grid was conceived more than a hundred years ago. This report brings together the perspective and experience of 13 Admirals and Generals of CNA's Military Advisory Board (MAB) to examine the grid through the prism of national security.

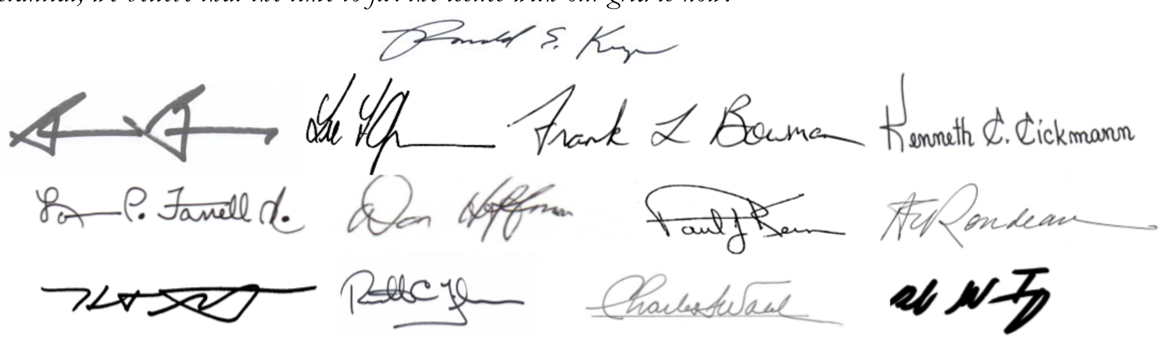
> **Failure to address known vulnerabilities and unwillingness to improve the grid aggressively—into one that is more adaptable, resilient, and reliable—hold the nation's security at risk.**

For a number of years now, we the members of CNA's MAB have analyzed energy security from a military perspective. One of our consistent findings is the need for secure, affordable, and resilient sources of power that can ensure mission accomplishment in the face of a determined adversary. This finding has led the Department of Defense (DOD) to pursue an energy program focused on reducing demand, diversifying supply, and considering energy implications in all decisions. DOD established this program to develop assured power for all operations.

Several well-publicized attacks and failures of parts of our national electrical grid led us to look more closely at vulnerabilities associated with that system and the effect failures would have on our national security here at home, including accessing the impact of grid failure on the ability of the DOD workforce to maintain installations, conduct training, and execute operations. In this respect, we found that DOD serves as a microcosm of the grid challenges facing our entire nation, while at the same time it provides insights into possible solutions. In military operations, we build forces with the principles of defense in depth, agility, distributed command and control, and redundancies to minimize single-point failures. We believe we must rebuild our electrical grid with similar constructs to prevent crisis, rather than just to respond.

We find ourselves at a unique point in history. On the one hand, we have an aging grid with increasing vulnerabilities and determined adversaries. On the other hand, we have advancing technologies and proven, innovative sources that are much more capable of producing electrical power closer to the consumer. We have the technology to build a grid that is more resilient and much less of a strategic target for adversaries, and at the same time more flexible to accept future technological advances.

Because our adversaries are determined and the threats to our electrical grid and national security are real and substantial, we believe that the time to fix the issues with our grid is now.



Executive Summary

The trends are clear. The current way Americans produce and distribute electricity is at increasing risk, while over the next half-century the way we produce and use energy will radically change. Just as the twentieth century was dominated by energy derived from oil and coal, the twenty-first century will see much greater energy diversity using solar, wind, small nuclear reactors, hydrogen, and other low-carbon sources.

The current U.S. electric grid's overreliance on aging twentieth-century technology—based on centralized power generation and interconnected distribution architecture—makes it susceptible to a wide variety of threats, including severe weather and other natural disasters, direct physical attack or cyberattack, and accidents associated with the age of the grid or human error. The national security vulnerabilities associated with the grid, its discrete power generation and nodal distribution, and the design of power transmission leave the U.S. open to both small/short-duration and large/long-duration power outages.

Between 2011 and 2014, electric utilities reported 362 targeted attacks that caused outages or other power disruptions. Of those, 14 were cyberattacks, and the rest were physical in nature [1]. While seldom publicized, the growing number of these attacks is a distressing trend. This trend requires us to consider the potential for even more serious assaults, with strategic consequences.

Assuring that we have reliable, accessible, sustainable, and affordable electric power is a national security imperative. Our increased reliance on electric power in every sector of our lives, including communications, commerce, transportation, health and emergency services, in addition to homeland and national defense, means that large-scale disruptions of electrical power will have immediate costs to our economy and can place our security at risk.

Whether it is the ability of first responders to answer the call to emergencies here in the United States, or the readiness and capability of our military service members to operate effectively in the U.S. or deployed in theater, these missions are directly linked to assured domestic electric power.

The vulnerabilities inherent in today's grid expose it to a one-two punch: First, cities and regions get their power primarily from large clustered electric power producers. Second, that electricity is typically transmitted over long distances, across vulnerable, high-voltage infrastructure. Nearly every part of the generation and transmission network is at risk to attack, weather, or other threats that could result in a sustained power outage to major cities or entire regions of the nation. With the grid of the future, electricity will be produced closer to consumers, from a wide variety of sources, and stored or shared until needed. The new production paradigm will be driven by technological advances, demand for increased flexibility, more secure and lower-cost power, and a growing public demand for cleaner energy sources.

Assuring that we have reliable, accessible, sustainable, and affordable electric power is a national security imperative.

In looking at the national security implications of assured electrical power, we applied our collective military experience and leveraged the numerous reports published by institutions such as the National Research Council, the Defense Science Board, the Department of Homeland Security (DHS), the Department of Energy, and others that highlighted the specific aspects and impacts of the grid's vulnerability, such as its effects on military installations or power transmission and distribution.

We found that we have an opportunity now to move America toward an advanced energy economy. Through public and private investment, forward-thinking action by policymakers and utilities alike, incentives, and strong public policy, we can modernize and design a reliable, secure grid to serve our nation for the next one hundred years. We can transition to a grid that not only is flexible enough to accept today's already proven alternative energy sources, but also one that accepts new, emerging technologies as they become available.

In the short and medium term, existing technologies such as micro-grids; proven distributed electrical generation systems such as wind, solar, and geothermal; and evolving systems that will use distributed electrical generation plants such as commercial-scale hydrogen engines, fuel cells, small modular reactors, and emerging energy storage systems can increase electrical generation and distribution security. These—and other—technologies, coupled with energy efficiency, have the ability to provide the United States with a more reliable and secure power supply.

Through public and private investment, forward-thinking action by policymakers and utilities alike, incentives, and strong public policy, we can modernize and design a grid to serve our nation for the next one hundred years.

In the long term, smart design and effective planning can ensure that critical research and development investments in advanced electric generation, storage, and emerging technologies can be incorporated smoothly into the grid without barriers or obstacles. A new, flexible, open-architecture grid paradigm will provide for electrical energy that is generated closer to the user and will be less of a strategic target. It will help end our reliance on traditional, environmentally damaging high-carbon fuels with unpredictable costs. More to the point, though, a well-designed electrical grid will reduce our reliance on large, vulnerable regional power plants and their highly exposed distribution infrastructure, thereby strengthening our national and homeland security.

Recognizing that the grid is a consolidation of many separate utilities forming a confederation of energy services, we believe it is important that there be a central direction toward which each utility can strive to achieve unity of effort and mutual security. We recognize that the policies governing and regulating most electrical utilities are made at the state and local levels, leading to a variety of complementary and differing approaches across the United States. To this end, common standards and planning tools are crucial for proper alignment.

Given the long life of the grid, we believe it is fair to say that decisions made now about the grid of the future will be reflected in the strength of our national defense and our country's way of life for decades to come. We, the members of the Military Advisory Board, offer the following recommendations to policymakers at all levels of government.

- **Develop a formal national strategy for strengthening the security and resilience of the electric grid through a "whole-of-government" approach at all levels—from the Nation's Capital, down to local governments.** The challenge of designing and implementing the grid of the future is that a whole-of-government effort is required (local, state, and federal) in assessment, planning, and execution, to avoid the development and implementation of incompatible approaches.

- **Examine and act to change misaligned government incentives and policy-based deterrents**. The role of government should be as a leader developing a roadmap, complete with short-, intermediate-, and long-term considerations and actions.
- **Incorporate an advanced energy economy strategy into all grid modernization, repair, and rebuilding efforts**. All projects—from individual rooftop solar panels to an extensive repair and replacement of electrical infrastructure after a natural disaster—must be aligned with a cohesive national strategy to move the nation forward. We must no longer simply rebuild our electric infrastructure to the way it was; we must rebuild it better.
- **Integrate stronger and smarter planning for adoption and roll-out of new grid technologies.** State and regional planning should allow for—as well as foster—opportunities for the adoption of new technologies that strengthen the security of our power supply. In the near term, state and regional electric power planning processes, models, and tools should be modified to include distributed generation and distribution applications, energy storage solutions, and smart-grid technologies into future planning and investment cycles.

- **Conduct quantitative risk analysis, including assigning monetary values for impacts associated with the complete set of threats to the grid.** Reducing risk provides a major incentive for change. More accurately quantifying the risks and vulnerability will provide consumers, utilities, and governments (at all levels) with the information needed to balance investments in, and development of, distributed electricity generation and distribution resources, energy storage capacity, and smart-grid technologies.
- **Seize the opportunity to build smarter, better, and cleaner.** By harnessing clean energy sources we can reduce the carbon footprint of individuals, businesses, and military missions. Designing and implementing a new grid built on the combination of distributed power generation and distribution, ample energy storage, and smart-grid technologies provides the opportunity to rely on clean and abundant energy resources.
- **Promote data collection, analysis, and transparency.** Power utility companies and decision makers need better access to data on the operating characteristics, costs, and the full range of benefits of various alternative systems to allow for equal and consistent comparison with central generation and other conventional energy resource options. Data on energy generation, transmission, and use can inform further development of smart-grid technologies and other advanced energy technologies. Innovation will be fostered when all parties (utilities, consumers, and regulators) have access and can make informed decisions based on transparent and readily available data.

- **Invest in the grid at a level commensurate with its strategic significance to our everyday lives.** Continue to expand investment in research and development of smart grids and energy efficiency, and in components hardened against the full spectrum of threats. Incentivize the development of technologies that will provide affordability and reliability of, and redundancies in, the grid of the future, while reducing its strategic vulnerabilities. Invest in U.S. manufacturing for critical components so we can be assured of supply and resupply, enhancing an advanced energy economy for generations to come.

The Grid and National Security: Why Now?

Our dependence on assured and reliable electric power has never been greater. As one example, look no further than digital communications, which are intrinsic to almost every aspect of our daily existence [2]. "Cloud computing" is on the rise, as is the emergence of "the internet of things." None of the major advances in information technology can be accessed without electricity. Similarly, the private sector and our military logistics networks communicate and operate in an environment driven by data systems that depend on reliable sources of electrical power.

Our dependence on assured and reliable electric power has never been greater.

Financial transactions are conducted electronically. Basic public utilities, including water supply systems and sewage treatment facilities, require electricity to run the control systems for the pumps and purification equipment. Our transportation systems, from traffic lights to air traffic control, require electrical power. Essential duties performed by emergency managers, law enforcement professionals, and healthcare providers require electrical power. Our day-to-day communications, whether through voice or digital stream—email, text, social media—require electrical power. Increasingly, all of our information and data for all sectors—governmental, medical, manufacturing, financial, and military—all are maintained electronically. The list goes on and on—through every aspect of our lives.

Although many of these sectors have backup power generators, the equipment and fuel reserves needed to keep the backups running are generally intended to be used for just hours or, at most, a few days. Also, these backup systems may provide power only to a limited number of essential operations. When power loss extends into days or weeks, these backup systems will begin to fail, communications and transportation functions will break down, and essential life-saving services will degrade. The likely resulting chaos and potential social unrest will present overwhelming challenges for emergency responders, law enforcement, and public health and medical providers—providers who will be confronting the same power shortages.

A Stacked Deck: Grid Susceptibility and Heightened Threats

Today's grid is built on the model that power comes from large stationary power-generation facilities, flows through hundreds of thousands of miles of transmission lines and high-voltage transformers, and finally reaches consumers (see Figure 1).[1] As the grid has evolved incrementally to meet the needs of our growing and increasingly urban population, power plants have grown in size and distance from consumers, and they have decreased in number [3]. Today's grid—actually comprising three grids: the Eastern, Western, and Texas Interconnects—is rigid. It is designed for power to flow in one direction. It has little flexibility and many vulnerable points of failure that can result in the collapse of large segments.

[1] Electric power transmission substations rely on large power transformers (LPTs) to adjust electric voltage as necessary to move power across the grid [3]. High-voltage transformers, a category of LPTs, represent only 3 percent of the substation transformers in the U.S., and yet they carry 60 to 70 percent of the nation's electricity [4]. Restoring LPTs, and in particular high-voltage transformers, requires a great deal of time (up to 21 months) and money (upwards of $3 to $5 million per unit) due to the limited availability of spare LPTs and LPT parts, the significant concentration of LPT manufacturers abroad, and the highly customized nature of these systems [5].

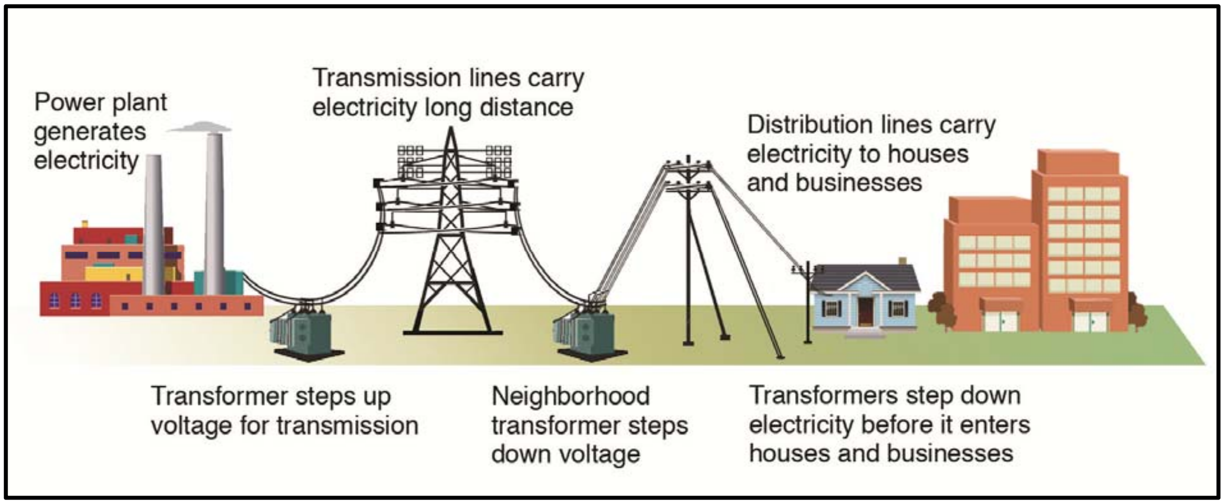


Figure 1. Electric power generation, transmission, and distribution

Within the transmission portion of the grid, there are 55,000 transmission substations,[2] and according to a Federal Energy Regulatory Commission study, the loss of just nine of these nodes could result in a regional or nationwide outage that could last for weeks or possibly months, with restoration delayed by lack of available replacements [6]. Power utilities are prepared to address events that take one or even two transformers offline, but a natural disaster or coordinated attack that severely damages or fully disables more than two transformers could result in cascading blackouts [8]. No federal rules require utilities to protect these substations unless they are connected to nuclear power plants.

In our 2009 report, *Powering America's Defense: Energy and the Risks to National Security* [9], we linked the vulnerability of the fragile domestic electricity grid to weather, accidents, and attacks, with the associated impacts on military installations.

... there are 55,000 transmission substations ... and the loss of just nine nodes could result in a regional or nationwide outage that could last for weeks or possibly months

In the six years since the release of the report, the risks associated with attacks—such as those by transnational terrorist groups (e.g., al Qaeda, ISIL/ISIS), adversarial governments, and "lone-wolf" perpetrators, as well as cyberattacks—have increased dramatically. Several recent incidents give us growing cause for concern, since they may be precursors of future threats.

Physical attacks

The design of the grid and its inherent vulnerabilities are known to our enemies—foreign *and domestic.*

2 In February 2014, the Federal Energy Regulatory Commission (FERC) internally disseminated the findings of its study on the national electric grid's security. Some of the findings were reported the following month in various major media outlets, including *The Wall Street Journal* [6]. In January 2015, the Department of Energy's Office of the Inspector General released the findings of its investigation of the media's publicizing such "nonpublic," sensitive information on the security of the nation's electric grid [7].

In 2013, the Pacific Gas and Electric (PG&E) Metcalf Transmission Substation located outside San Jose, CA, was the target of a sophisticated sniper attack. The Metcalf Substation supplies power to Silicon Valley, an American landmark of innovation. During the attack, gunmen fired on and disabled 17 transformers, causing $15 million worth of damage. The attackers have not been apprehended and their ultimate purpose remains unknown. The Federal Bureau of Investigation ruled out terrorism, but various independent investigations of the attack have pointed to its high degree of "sophistication." Some investigators concluded that the Metcalf Substation incident was a "dress rehearsal" for other attacks on a much larger portion of the grid [10] [11].

Although the Metcalf incident was one of the most coordinated attacks on a substation to date, attacks on substations are not isolated. In 2013, shots were fired at grid infrastructure in eastern Colorado, while two years earlier an individual broke into a critical hydro-electric converter station in Vermont with threatening intent. The individuals involved in all of these incidents remain at large [12].

The design of the grid and its inherent vulnerabilities are known to our enemies—foreign *and domestic*

Cyberattacks

Sophisticated cyberattacks with physical impacts have also been repeatedly identified as a major threat to the electrical grid [9]. Some experts infer that the threat of such attacks is overstated, while others point to the growing sophistication of cyberattacks and the proven ability of hackers to penetrate critical government systems such as those of the Office of Personnel Management (OPM) or the Department of Veterans Affairs (VA), and say that a major cyberattack is overdue. Unlike the OPM or VA attacks, it is not just data that is vulnerable on the grid. Our power infrastructure relies on automated and centralized control systems. Cyberattacks designed to disrupt or divert the flow of electricity and vital information, deactivate protective systems, dump energy stores, or transmit false signals to operators can result in cascading effects that could have serious long-term damaging impacts or amplify the damage from physical attacks [13]. Or they could be openings to much more extensive—and devastating—attacks.

In 2008, a CIA official revealed that hackers penetrated power systems in several regions outside the United States, and in one case, "caused a power outage affecting multiple cities" [13]. Cyberattacks are becoming more deliberate and more effective, particularly as innovative technologies open the door for greater remote access to grid systems, and as potential saboteurs become more sophisticated at understanding the impact of shutting down critical infrastructure.

Weather

It is not just targeted attacks that are of concern. Currently, severe weather events are the leading cause of power outages in the United States. Between 2003 and 2012, severe weather was responsible for an estimated 679 widespread power outages in the United States (e.g., outages affecting 50,000 or more customers) [14]. The impacts of past power outages over a significant geographic area provide some insight into the potential consequences of a prolonged, widespread electrical power outage. Just over a decade ago, in August 2003, a weather-related disruption in the northeastern U.S. and a portion of Canada was responsible for a two-day electrical power loss.

This cascading blackout left retail and banking outlets; transportation systems, including road and rail; phone service; and radio broadcast and other communications systems offline and in the dark for days. The two-day event resulted in 50 million people without power, an estimated $6 billion in costs, and at least 11 deaths [9].

Other noteworthy examples include outages from Hurricanes Katrina and Rita, and Superstorm Sandy. Superstorm Sandy indirectly caused 50 deaths attributed to power outages alone. Because fuel distribution facilities didn't have power after Superstorm Sandy, U.S. military forces were used to procure and deliver 24 million gallons of fuel to staging areas in the storm-impacted area for distribution by the Federal Emergency Management Agency (FEMA, part of DHS) [15]. Delivering fuel prevented these military forces from performing other, perhaps even more critical defense support to civilian authority missions. The extensive grid damage from Hurricanes Katrina and Rita required months to repair, further hampering response and recovery efforts.

Prolonged widespread electrical outage would impact numerous domestic installations, placing at risk domestic military operations and those in-theater conducing combat, humanitarian, and other operations.

While not traditionally in the public eye, space weather events such as strong auroral currents, coronal mass ejections, and geomagnetic storms also pose significant risk to the grid. A 2011 DHS study describes the risk of widespread and sustained grid damage resulting from space weather events, and classifies these risks as a national security issue. Further, in 2008 the National Academy of Sciences unambiguously concluded that strong auroral currents can disrupt and damage electric power grids [16]. For an example of space weather impacts, look no further than the collapse of northeastern Canada's Hydro-Quebec power grid during a 1989 geomagnetic storm, which left millions of people without electricity for hours. Under our current grid design, we could expect similar impacts in major U.S. cities.

Aging infrastructure

Accidents stemming from the difficulty in maintaining aging energy infrastructure have also resulted in power outages. A few of the more significant recent examples include:

- April 2015—faulty equipment at a power switching station in rural Maryland was responsible for widespread power outages that impacted a significant portion of the metropolitan Washington, DC area, including the White House and State Department [17]
- October 2014—an explosion in the Manchester Street Power Station caused widespread power failures across downtown Providence, RI
- March 2012—a fire in Boston Back Bay transformers caused widespread power outages, and compelled authorities to close subway stations, block roads, and conduct evacuations.

Other age-related failures occur with uncomfortable regularity, from small rural towns to megacities.

Power Loss: Direct Impact on National Defense

As highlighted in our report, *Powering America's Defense*, military installations across the country rely heavily on the same grid as our communities, towns, and cities. The Department of Defense (DOD) requires a reliable and secure power supply for a multitude of critical systems that must be online every hour, every day, year-round. For example, our land-based Ballistic Missile Defense systems are critical to protecting our homeland 24/7.

At the same time, numerous command-and-control headquarters provide support to forward bases. These installations receive and analyze threat data, provide direction and support to forward-operating forces, and stand ready to respond to threats or other calls to action from the United States or from our allies. Increasingly, remotely piloted vehicles and other direct support for remote battlefield operations are controlled from military bases here in the United States. Despite the military's redundant systems for critical operations and logistics, a prolonged widespread electrical outage would impact numerous domestic installations, placing at risk domestic military operations and those in-theater conducing combat, humanitarian, and other operations.

Although most military installations have backup power generation capabilities, these generators rely predominately on fossil fuel–based generators (i.e., diesel, propane, JP-8). To date, the Defense Department has always been able to procure and transport the fuel it needs to domestic and overseas installations. However, under the scenario of a prolonged large-scale electrical power outage, if the commercial transportation sector comes to a standstill—as it likely will—there is the risk that the supplies needed to keep the military's domestic backup power equipment running may not be available. The Defense Science Board noted that "the military's backup power is inadequately sized for its missions and military bases cannot easily store sufficient fuel supplies to cope with a lengthy or widespread outage" [18]. Even accessing the U.S. Strategic Petroleum Reserve may be problematic if U.S. refineries do not have the needed electrical power to operate.

Military installations are not the only concern. Most of the active-duty military, civilian, and contract personnel supporting military operations live in communities surrounding the installations. In the event of a widespread power outage, critical personnel may not be able to report to work because they have transportation problems or because they may be addressing emergency situations with their own families and neighbors. Mission effectiveness can be maintained only when the personnel who perform vital mission functions are able to report to work and operate productively without distraction. The installations where these people work may have backup power, fresh water, medical services—and they will be able to operate temporarily during a grid failure—yet they do not have the capacity to serve as safe havens for surrounding communities while maintaining mission effectiveness, nor to unburden operators worried about their families at risk.

A Plan to Prevent—Not Just a Plan to Respond: Innovations and Open Architecture

The vulnerabilities and risks inherent in the current U.S. electrical grid demand a new approach to our nation's power paradigm, but they are not the only impetus to begin the process of building the grid of the future now. Technological advancements in distributed power generation, power distribution, energy storage, and "islanding" architecture—coupled with the wide range of available energy sources—make the development of new, resilient, reliable, clean, and affordable modern electricity systems not only *possible* but, in the our assessment, *imperative*. In building the grid (or grids) of the future, there is the opportunity to strengthen national security while protecting and even improving the American way of life.

The vulnerabilities and risks inherent in the current U.S. electrical grid demand a new approach to our nation's power paradigm

The current grid is aging and requires major investment to replace old and obsolete equipment. It is currently characterized by both its centralized generation nodes and its limited interconnected transmission infrastructure. At the same time, this distribution infrastructure has developed into a complex array of substations and high-voltage transmission lines that transform and move power over great distances to local distribution networks with many critical control points. To merely maintain the status quo while accommodating our nation's growing demand for electricity and ancillary service will require large-scale investments from both the private and public sectors. The American Society for Civil Engineers has identified an annual $10 billion investment gap projected over the next ten years [19]. As utilities and state/local regulators determine their investment strategies on how to close this gap, the question is: Why not invest smartly and build a better grid that is more resilient, more reliable, and more secure?

The development of tomorrow's grid must enable tomorrow's energy source mix, incorporating evolving energy storage and distribution systems, as well as distribution management and control technologies. For many individuals, communities, and commercial consumers, the grid of the future will be not just a place where they can get electricity, but also a place where they can store the electricity they have produced from their own energy sources. The new grid must be built knowing that technology will evolve even more rapidly during the next century than the last. Hence our investment in the new grid must have an open architecture, where new technologies can be "plug and play."

Tomorrow's grid must enable tomorrow's energy source mix, incorporating evolving energy storage and distribution systems, as well as distribution management and control technologies

From our perspective as members of the CNA Military Advisory Board, the grid of the future should look more like successful military forces: flexible, agile, and dispersed, with distributed operations (including command-and-control) and defense in depth.

The Future Is Now

As military leaders, we have significant experience examining trends, weighing uncertain future events, and deciding when it is time to act. We see an aging, increasingly vulnerable electrical grid in the light of a growing number of threats to our homeland and national security, but we also see many technologies that already provide solutions, and other remedies on the verge of technological breakthroughs. Below we highlight examples of some of these proven technologies and others with the potential to revolutionize the provision of electricity in the United States. After careful consideration of the state of America's electrical grid, we are convinced that the time to act is now.

Distributed Generation

Distributed generation (DG) places the source of electricity closer to those who need it. It is an alternative to what we traditionally think of as a large power plant supplying electricity to a city or region. DG offers flexibility—more choice in energy sources, choice that can be driven by availability of local resources, costs, or ease of access. The diversity of supply that can be applied through the distributed generation model improves reliability by eliminating single-point failures. DG can also lower the vulnerabilities associated with long transmission lines and associated high-voltage transformers. As technology advances, the range of available DG options will grow.

After careful consideration of the state of America's electrical grid, we are convinced that the time to act is now

The most significant recent developments allowing us to move toward more secure energy production capabilities have been in the area of distributed generation. Current distributed generation technologies include solar, wind, and water-powered energy systems; internal combustion engines running on either renewable or fossil fuels; combined heat and energy systems; and small gas turbines, micro-turbines, fuel cells, geothermal energy systems, tidal systems, or other small-scale hydroelectric mechanisms, to name a few. In the very near future, we see the potential commercial application of small modular reactors, solid oxide fuel cells, and other more advanced and innovative technologies. In addition to increasing grid reliability, most of these systems also move us closer to a clean-energy economy. To help appreciate the pace of these DG trends, we offer two of these technologies as examples: solar power and small modular reactors.

Driven by cost reductions associated with economies of scale, innovative financing, and investment tax incentives, solar power in the United States has grown nearly tenfold in the last five years. According to the U.S. Energy Information Administration, the U.S. generated nearly 20 gigawatts (GW) of solar power in the last year—enough to power more than four million homes [20]. In 2014, utility-scale solar grew by 38 percent, adding more than 4 GW, while the residential sector added 1 GW, growing by 51 percent [20]. While residential installation costs have dropped by 45 percent since 2010, utility-scale costs have dropped even more significantly, with recent contracts at prices below $0.05/kilowatt-hour (kWh)—on par with conventional power-plant pricing. Developments in solar power are innovative, and over the coming decades we expect to see continued improvements in solar technology: Collectors will gather energy from a wider swath of the solar spectrum; panels will be flexible and more transparent, with a far greater range of application, and they will increasingly become a main component of new residential/commercial construction (instead of an after-market add-on). In the not too distant future every American will own some solar device, whether it's to charge a night light, a garden decoration, or an entire home.

The most significant recent developments allowing us to move toward more secure energy production capabilities have been in the area of distributed generation

On the other end of the scale of emerging distributed generation technology are small modular reactors (SMRs). SMRs are nuclear power plants that are small in size (300 MW or less), compact in design, and factory-fabricated—requiring little to no construction work on site. SMRs offer the advantage of lower initial capital investment, scalability, and flexibility to be used at locations not suitable for larger nuclear reactors. They hold the promise of enhanced safety and security, and much wider distribution across the country.

As of mid-2013, there were 45 SMR concepts in various stages of research and development worldwide, with at least four under development in the United States [21]. Small reactors have successfully and safely powered hundreds of U.S. Navy ships and submarines for more than 60 years. Most SMRs can be built below the surface of the ground for safety and security, lowering vulnerabilities to man-made and natural threats. In an open-architecture grid system, SMRs could be built and quickly added where needed. The Defense Science Board is currently studying SMRs and how they could be used to improve the reliability of power to remote bases for the Department of Defense.

Not every location may be well suited for solar, SMRs, or other DG sources. The point we want to emphasize here is that there are scores of small electricity generation systems already developed or being developed that may work in various locations and must be accommodated in an integrated electrical grid of the future. The challenge is building a grid capable of plugging the full range of generating capacity into the system.

Energy Storage

Energy storage provides the means to efficiently capture excess electrical energy when production exceeds demand, and to "power shape" throughout the demand cycle. When it comes to electrical storage, most people think of batteries, but that is only one type of storage device. Today we can store excess electrical energy using a wide variety of methods, most requiring some type of conversion, for example:

- kinetic energy—flywheel or spinning disc
- potential energy—pumped hydro or compressed gas
- chemical energy—batteries and synthetic fuel production, including hydrogen or methanol production
- direct electrons—capacitors and ultra-capacitors.

While existing energy storage technologies can accommodate much of the distributed generation capacity for the next decade or more, advanced energy storage is a future requirement for meeting the full potential of a secure and resilient grid. As energy generation becomes more diverse, meeting varying demand with higher power quality may become more challenging. The grid of the future must be able to accept energy storage advancements, ranging from the proven technologies of today such as simple flywheels, hydro-pumping, and residential batteries to cutting-edge developing technologies using advanced electrolytes, nano-structured electrodes, and carbon tubes for building ultra-capacitors.

Advanced energy storage systems may make the grid more of a network to store and distribute electricity locally, rather than one to produce and transmit electricity

Because the power production of some of today's distributed generation sources varies over time, having accessible energy storage has been a factor in these sources' acceptability. Significant investment has already been made by the public and private sectors in developing residential, scalable energy storage systems that have reached the point of commercial viability. But this need not be a case where "one size fits all." The future grid must be built to accept a variety of storage systems. Although today's storage capability may continue to support much of the distributed generation for the coming years, in some areas acceptance appears to be more a challenge of policy rather than capability.

Nonetheless, the trend in advanced energy storage is clear: nanotechnology, advanced manufacturing, and applied innovative concepts such as carbon tubes being used to build ultra-capacitors, safer hydrogen storage facilities and other fuel cell or synthetic fuel–related storage systems, and other new approaches to energy storage may radically change our ability to use the new grid. Advanced energy storage systems may make the grid more of a network to store and distribute electricity locally, rather than one to produce and transmit electricity across great distances.

Micro-grids

Micro-grids are local, small-scale grids that can disconnect from the traditional grid to operate autonomously. A cruise ship is a perfect example of a micro-grid: in port, the ship plugs in and draws from the grid, but at sea it disconnects from the main grid and produces its own electricity for thousands of passengers, crew, and ship's operations. When a micro-grid separates from the main grid, it is an "island." Micro-grids strengthen resilience and help mitigate grid disturbances, because they are able to "island" and continue operating even while the main grid is down. They can also function as a resource for faster main-system response and recovery, as well as reduce energy losses in transmission and distribution. Micro-grids employ the principles of agility and flexibility; they can be used to more efficiently integrate new sources of distributed energy and energy storage to respond to variable demand.

Micro-grids are already being employed around the nation and around the world, from buildings to university campuses to entire communities and forward-operating military bases

Enabled by improved distributed power generation capabilities such as combined power and heat systems, photovoltaic (PV) solar and solar collectors, and wind—and using storage systems like advanced lithium hydroxide batteries, compressed air storage, pumped hydro and others—micro-grids are providing consumers and utilities with numerous advantages. Micro-grids can provide energy efficiency, lowered overall energy consumption, reduced environmental impact, improved supply reliability, and supply security. They can also aid in more cost-efficient electricity infrastructure replacement.

The Department of Energy (DOE) is advancing an aggressive program and several demonstration projects showing the viability of micro-grids and advanced micro-grid concepts. One example is the Smart Power Infrastructure Demonstration and Energy Reliability and Security (SPIDERS) project, a Joint Capability Technology Demonstration between the Departments of Energy, Defense, and Homeland Security [22]. SPIDERS is focused on demonstrating secure micro-grid architecture with the ability to maintain operational confidence through trusted, reliable, and resilient electric power generation and distribution on military installations. It uses a standardized design approach and provides contracting, installation, security, and operation for three micro-grids under construction—each with increasing capability and complexity—at Camp Smith, NY; Fort Carson, CO and Joint Base Pearl Harbor–Hickam, HI. The three demonstration projects will promote:

- energy reliability for critical missions;
- high readiness and immediately deployable technologies; and
- cybersecurity for the control systems.

Another example, this one showing how local governments are embracing the concept, is the Pecan Street Project near Austin, TX.

Pecan Street Project

The University of Texas, in collaboration with Pecan Street, Inc., has successfully employed an innovative micro-grid in the community of Mueller, TX [23]. This 711-acre mixed-use project in a suburb of Austin is an effort to redevelop a location affected by the Base Realignment and Closure process [23] [24]. As a U.S. Department of Energy demonstration project, the Pecan Street Project developed and implemented an open-platform Energy Internet Demonstration [24]. According to Pecan Street's partners:

> The Energy Internet is the smart grid of the future, in which information flows between the utility and its customers, a web of interconnection exists within the home or business though devices embedded with intelligence that enable real-time management of the home's consumption and that enable aggregated energy management by the utility, enabling utilities to more efficiently balance demand and supply with clean energy sources without disrupting their customer's quality of life [24].

The Pecan Street Project employed smart grid systems, including automated meter information, automatic meter reading (AMR) and advanced metering infrastructure (AMI) smart meters, home energy management systems (HEMS), distributed generation systems, intelligent load control, and advanced billing platforms [24]. The project provided unparalleled data on consumer energy use. The community adopted solar power and electric vehicles far above observed average adoption rates elsewhere, and allowed for the collection of energy usage pattern data. The data generated and collected in the project provides researchers with insight on micro-grids, smart-grid applications, distributed generation platforms, energy storage technologies, and energy use at the residential level.

At the state level, Massachusetts released a grid modernization plan in June 2014, establishing a platform for the state's utilities "to innovate and get the grid ready for more micro-grids, energy efficiency, distributed generation, electric cars, and other hallmarks of a new electric age." New Jersey has allocated $25 million to 146 state agencies "to develop micro-grids and other projects that improve the state's energy resiliency."

Micro-grids can provide energy efficiency, lowered overall energy consumption, reduced environmental impact, improved supply reliability, and supply security

New York State's Public Service Commission is finalizing details for the state's "Reforming the Energy Vision" (REV) plan, specifying the role of a statewide grid operator that "manages distributed energy much the way independent system operators now manage bulk power markets in the United States." The new "Distributed System Platform Provider" would serve as an exchange "where regulated and competitive distributed energy players buy and sell. The distributed grid operator would create markets, tariffs, and systems to monetize energy efficiency, micro-grids, combined heat and power, energy storage, demand response, distributed generation, building management systems, and other forms of distributed energy." The New York State REV plan "specifically calls out micro-grids as an element of distributed energy in need of policy attention" [25].

Smart Grids

The smart grid adds two-way digital communication technology to devices associated with the grid. It can connect consumers and producers, allowing consumers to have a greater input on demand signals associated with price or capacity fluctuation. For example, consumers can set a price cap on how much air conditioning power to buy at a given time during the day. Each device on the network can be given sensors to gather data (power meters, voltage sensors, fault detectors, etc.), and can have two-way digital communication between the device in the field and the utility's network operations center.

If done smartly, and with appropriate cyber protections, a smart grid will improve reliability, resiliency, flexibility, and efficiency (both economic and energy) of the electrical power delivery system. Examples include self-repair from power disturbance events, enabling active participation by consumers in demand response, operating resiliently against physical and cyberattack, and providing power quality for twenty first–century needs.

Smart micro-grids, combined with distributed generation and evolving energy storage capabilities, can be the basis of a flexible, secure, and resilient approach to a reliable supply of electricity.

Department of Defense: Test Bed for the New Grid

In partnership with the private sector and academia, the Department of Defense has spurred innovation to improve the warfighter's ability to meet mission demands and has served as a driving force of technological change. DOD's projects in the aerospace, robotics, energy, transport, and logistics sectors have produced many of the nation's technological breakthroughs, providing the private sector with the foundation for growth and large-scale adoption of new technologies. When it comes to the future of electrical energy, DOD is again playing an important role as it leads by example in advancing renewable, distributed energy generation. DOD has a goal of consuming 20 percent of its energy from renewable sources by 2020 and producing 3 GW of renewable energy from distributed sources by 2025, at installations and in the field [26].

The deployable and decentralized energy production afforded by renewable sources and by technologies like micro-grids and energy storage systems can improve the safety, security, and effectiveness of the military. Renewable energy and efficiency improvements can increase warfighter capability; improve the energy security of DOD installations; and cut energy costs, freeing valuable resources for other capabilities.

Renewable, distributed energy is not just a "policy objective" for the U.S. military, it is an operational *imperative*

To this end, DOD has more than 1,130 distributed, stationary electrical power generation sources using renewable energy, generating more than .5 GW of power (not including ships, submarines, or other mobile platforms with generating capability). DOD generates most of its renewable electric power from geothermal and municipal solid waste power plants. It also has

DOD RENEWABLES

To meet its 3 GW goal of renewable power generation, DOD will embrace distributed generation across many of its installations and pursue a combination of production, power purchase, and unused land leases for utilities to generate energy derived from renewable sources. For example, in February 2014, DOD opened its largest land-lease solar project, a 16.4 MW PV array at Davis-Monthan Air Force Base (AFB), AZ. This outsized its next largest, 14.2 MW solar power production project at Nellis AFB in Nevada. DOD is also adding to its 270 MW of renewable production by constructing a 13.2 MW solar project at Naval Air Weapons Station China Lake, CA. This PV array will add to the 170 MW of geothermal electricity already being produced there. All of these PV projects will fall short of the 20 MW solar array approved by DOD for installation at Fort Bliss, TX [26].

more than 645 solar photovoltaic (PV) systems in nearly every state and territory from Alaska to Florida that contribute approximately 11 percent of the total renewable energy produced [26]. It is adding more every day.

In addition to producing electricity, DOD is testing the implementation of micro-grids to obtain increased reliability at an overall lower cost (networking requires fewer generators); greater efficiency, which also provides cost savings (networking allows for load sharing); ready integration of renewable energy source generation, which provides energy security; reduced costs through demand-response programming and peak-sharing; and financial gains by leveraging ancillary services. Military bases are using micro-grids, energy storage, and ancillary-service markets at Marine Corps Air-Ground Combat Center, Twentynine Palms, CA; Fort Bliss, TX; and Joint Base McGuire-Dix-Lakehurst, NJ as demonstration projects [27]. In addition to solar power generation, Tinker AFB, OK and Robins AFB, GA have collaborated with local utilities to develop islanding capability by installing combustion gas turbines with dual fuel capability. Fort Detrick, MD and Naval Surface Warfare Center Dahlgren Division, VA generation resources can synchronize and operate in a parallel with the grid or in an islanded mode [27].

DOD TACTICAL ENERGY

The application of innovative energy solutions is not exclusive to domestic DOD installations. Solar energy generation currently enhances the "tactical edge" and security of deployed forces. Using portable solar arrays, forward units have successfully supplied power to "fixed-site" locations, many of which are remote and beyond the reach of an electrical grid. In addition to meeting the austere conditions of the environment, portable solar generation applications also reduce the need for traditional liquid fuel–based generators forward, thereby reducing the number of risky fuel resupply missions. Forward-deployed soldiers' ready acceptance of renewable energy generation capabilities provides strong evidence of their reliability. Soldiers have to trust the gear with which they enter the theater, because their lives depend on it. They have embraced solar power as a means to lower reliance on long logistic tails, reducing the number of fellow soldiers whose lives are placed at risk.

Summary

The U.S. electrical grid must change.

Short-, intermediate-, and long-term investments in research and development in a twenty first–century energy infrastructure are essential. The new grid must be resilient and able to withstand multiple accidents or attacks without the catastrophic collapse and associated cascading impacts affecting entire regions and major portions of the population. The new grid's design must incorporate open, distributed, and isolatable architecture concepts, and possess the flexibility to accept and store energy from a variety of sources, including those yet to be fully developed. The new grid must be reliable, with the ability to "island off" large and small sectors when other segments fail.

We also fully recognize that there has been significant investment in the current model of electricity production and distribution in both the infrastructure and the policies that make the business of electricity work. Changing to a new twenty first–century grid requires both public and private investment; this kind of investment will strengthen both our homeland and national security, and will create an environment where new innovations in energy and clean technology can strengthen our economy. Continuing to rely on the current grid simply is not an option.

As senior military leaders, we have learned not only to accept change but to embrace it and to use it for strategic or operational advantage. Adopting technology and the ensuing change in operations has been a hallmark of U.S. military success. The inevitable modifications to the U.S. electric grid must be driven by thoughtful and informed policymakers, planners, and utilities, willing to act on security risks that are not well-defined and to some degree remote, but nevertheless very real. The actions of thoughtful leaders today will head off the potential of an unthinkable future crisis in the supply of electrical power to this country. They must work now to develop the governmental and private-sector investment and cooperation necessary to ensure that our nation's electricity grid will not falter—now or in the future. Too much is at stake.

Admiral Frank "Skip" Bowman, USN (Ret.)
Former Director, Naval Nuclear Propulsion Program;
Former Deputy Administrator–Naval Reactors, National Nuclear Security Administration

For over eight years, Admiral Skip Bowman was Director, Naval Nuclear Propulsion, Naval Sea Systems Command, and concurrently Deputy Administrator for Naval Reactors in the Naval Nuclear Security Administration, Department of Energy. Also as a flag officer, Admiral Bowman served as Chief of Naval Personnel and as Director for Political-Military Affairs and Deputy Director for Operations on the Joint Staff.

He was commissioned following graduation in 1966 from Duke University. In 1973, he completed a dual master's program in nuclear engineering and naval architecture/marine engineering at the Massachusetts Institute of Technology, and was elected to the Society of Sigma Xi. Admiral Bowman has been awarded the honorary degree of Doctor of Humane Letters from Duke University.

Admiral Bowman was President and CEO of the Nuclear Energy Institute from 2005 through 2008. NEI is the policy organization for the commercial nuclear power industry. In 2006, Admiral Bowman was named an Honorary Knight Commander of the Most Excellent Order of the British Empire by Queen Elizabeth II. Admiral Bowman currently serves on the boards of directors of BP plc and Morgan Stanley Mutual Funds.

Lieutentant General Ken Eickmann, USAF (Ret.)
Former Commander Aeronautical Systems Center, Wright-Patterson AFB

From 1996 to 1998, General Eickmann served as the Commander, Aeronautical Systems Center, Wright-Patterson AFB, where he led the nation's largest center of excellence for research, development, and acquisition of aircraft, aeronautical equipment, and munitions. General Eickmann was the Commander of the Oklahoma City Air Logistics Center and Installation Commander of Tinker Air Force Base from 1994 to 1996; Deputy Chief of Staff for Logistics and Chief of Staff for Air Force Materiel Command from 1992 to 1994; and DCS Logistics, Headquarters Pacific Air Forces from 1990 to 1992. The General served six years on the Air Force Science and Technology Board and has chaired numerous energy-related studies for the National Academy of Sciences and the National Research Council. He is a recognized expert in energy, logistics, and propulsion technology, and has published several papers in technical journals in the U.S. and overseas.

General Eickmann is currently the Deputy Director of the Center for Energy Security at the University of Texas in Austin. He holds a bachelor's degree in Mechanical Engineering from UT Austin, a master's degree in Systems Engineering from the Air Force Institute of Technology, and is a graduate of the University of the Michigan School of Business and the John F. Kennedy School of Government, Harvard University.

Lieutenant General Lawrence P. Farrell Jr., USAF (Ret.)
Former Deputy Chief of Staff for Plans and Programs, Headquarters USAF

In 1998, General Farrell served as the Deputy Chief of Staff for Plans and Programs, Headquarters U.S. Air Force, Washington, DC. He was responsible for planning, programming, and manpower activities within the corporate Air Force, and for integrating the Air Force's future plans and requirements to support national security objectives and military strategy. Previous positions include Vice Commander, Air Force Materiel Command, and Deputy Director, Defense Logistics Agency. He also served as Deputy Chief of Staff for Plans and Programs at Headquarters U.S. Air Forces in Europe. A command pilot with more than 3,000 flying hours, he flew 196 missions in Southeast Asia, and commanded the 401st Tactical Fighter Wing, Torrejon Air Base, Spain.

General Farrell is a graduate of the Air Force Academy with a BS in Engineering, and an MBA from Auburn University. Other education includes the National War College and the Harvard Program for Executives in National Security.

Brigadier General Gerald E. Galloway Jr., USA (Ret.)
Vice Chairman, CNA Military Advisory Board
Former Dean at the United States Military Academy, West Point; and Dean at the Industrial College of the Armed Forces, National Defense University

Brigadier General Gerry Galloway served for 38 years as a combat engineer, civil engineer, and a military educator in various command and staff assignments in Germany, Southeast Asia, and the United States before retiring in 1995. He is currently a Glenn L. Martin Institute Professor of Engineering and an affiliate Professor of Public Policy, University of Maryland, where his research focuses on disaster risk management and the impacts of climate change in the U.S. and internationally. He commanded the Corps of Engineers Vicksburg Engineer District and was a Presidential appointee to the Mississippi River Commission from 1988 to 1995. From 1994 to 1995, he was assigned to the White House to lead a committee in assessing the causes of the 1993 Mississippi River flood. In 2006 he chaired an Interagency National Levee Policy Review Team. Since 2010 he has served on the Governor of Louisiana's Advisory Commission on Coastal Protection and Restoration.

He is a graduate of the U.S. Military Academy and holds master's degrees from Princeton University, Pennsylvania State University, and the U.S. Army Command and General Staff College; he also holds a doctorate from the University of North Carolina at Chapel Hill. He is a member of the National Academy of Engineering, has served on thirteen committees of the National Research Council, chairing two studies of future Army logistics, and is a member of the National Academies Roundtable on Risk, Resilience, and Extreme Events.

Vice Admiral Lee F. Gunn, USN (Ret.)
Vice Chairman, CNA Military Advisory Board
Former Inspector General of the Department of the Navy

Vice Admiral Lee Gunn served for 35 years in U.S. Navy. His last active duty assignment was Inspector General of the Department of the Navy, where he was responsible for the department's overall inspection program and its assessments of readiness, training, and quality of service. Serving in the surface Navy in a variety of theaters, Gunn rose through the cruiser/destroyer force to command the frigate USS *Barbey*, then commanded the Navy's anti-submarine warfare tactical and technical evaluation destroyer squadron, DESRON 31. He later commanded Amphibious Group Three. As Commander of PHIBGRU THREE he served as the Combined Naval Forces Commander, and Deputy Task Force Commander of Combined Task Force United Shield, which conducted the withdrawal of UN peacekeeping forces from Somalia.

Gunn holds a bachelor's degree in experimental and physiological psychology from the University of California, Los Angeles, and a master of science degree in operations research from the Naval Postgraduate School in Monterey, CA.

General Donald J. Hoffman, USAF (Ret.)
Former Commander, Air Force Materiel Command

General Hoffman retired in June 2012 after managing a workforce of 80,000, with a $60 billion budget to develop, acquire, test, and sustain Air Force weapon systems. He also served as the Military Deputy for Air Force Acquisition in the Pentagon and the Director of Requirements at Air Combat Command. He is pilot with over 3,800 hours in fighter, trainer, and transport aircraft, and has served in numerous operational commands.

A graduate of the U.S. Air Force Academy, General Hoffman has a master's degree in electrical engineering from the University of California, Berkeley, and has attended the National War College and the National Security Management Course at Syracuse University.

General Paul J. Kern, USA (Ret.)
Former Commanding General, U.S. Army Materiel Command
Chairman, CNA Military Advisory Board

General Kern was Commanding General, Army Materiel Command from 2001 to 2004, and Senior Advisor for Army Research, Development, and Acquisition from 1997 to 2001. He was commissioned as an Armor Lieutenant following graduation from West Point in 1967 and served three combat tours—two in Vietnam as a platoon leader and troop commander, and the third in Desert Shield/Desert Storm. In the 1990s, Kern served as Senior Military Assistant to Secretary of Defense William Perry. In June 2004, at the request of Secretary of Defense Donald Rumsfeld, Kern led the military's internal investigation into the abuses at the Abu Ghraib prison in Iraq.

He holds master's degrees in both civil and mechanical engineering from the University of Michigan, and was a Senior Security Fellow at the John F. Kennedy School of Government at Harvard University.

General Ronald E. Keys, USAF (Ret.)
Former Commander, Air Combat Command

General Ron Keys retired from the Air Force in November 2007 after completing a career of over forty years. His last assignment was as Commander, Air Combat Command—the Air Force's largest major command, consisting of more than 1,200 aircraft, 27 wings, 17 bases, and 200 operating locations worldwide with 105,000 personnel. General Keys holds a bachelor of science degree from Kansas State University and a master's degree in business administration from Golden Gate University. General Keys is a command pilot with more than 4,000 flying hours in fighter aircraft, including more than 300 hours of combat time.

No stranger to energy challenges, General Keys first faced them operationally as a young Air Force Captain, piloting F-4s during the fuel embargo of the 1970s. Later, as Director of Operations for U.S. European Command, fuel and logistic supply provisioning were critical decisions during humanitarian, rescue, and combat operations across EUCOM's area of responsibility, including the Balkans and deep into Africa. As Commander of Allied Air Forces Southern Europe and Commander of the U.S. 16th Air Force, similar hard choices had to be made in supporting Operation Northern Watch in Iraq, as well as for combat air patrols and resupply in the Balkans. Later, as the Director of all Air Force Air, Space, and Cyber mission areas, as well as operational requirements in the early 2000s, he saw the impact of energy choices on budget planning and execution, as well as in training and supporting operational plans in Iraq and Afghanistan. Finally, at Air Combat Command, he faced the total challenge of organizing, training, and equipping forces at home and deployed to balance mission effectiveness with crucial energy efficiency. Continuing after retirement, he is a member of the Center for Climate and Security's Climate and Security Working Group, focused on developing policy options and encouraging dialogue and education on the issues. As a member of the CNA Military Advisory Board on DOD Energy Security and Climate Change projects, he is intimately familiar with the relationship of energy, military, economic, and national security.

General Keys owns RK Solution Enterprises, an independent consultancy. In addition to his energy portfolio, he is a Senior Advisor to the Bipartisan Policy Center, and a member of the Embry-Riddle Aeronautical University Board of Trustees.

Vice Admiral Ann Rondeau, USN (Ret.)
Former President of National Defense University
Former Deputy Commander, U.S. Transportation Command

Ann Rondeau served in the United States Navy, attaining the rank of Vice Admiral. Her last active duty assignment was President, National Defense University (NDU). Rondeau served in leadership, staff, and command assignments in myriad mission areas: fleet operations (anti-submarine warfare, air operations, operational intelligence, maritime transportation and sealift), strategy and policy, policy planning, strategic logistics, operations analysis, training and education, workforce development, business enterprise and installations management. She is currently an independent consultant with IBM's leading edge cognitive computing project, The Watson Group.

She has been active with the National Defense Transportation Association. She serves as Vice Chair, Board of Trustees, American Public University System, a subsidiary of American Public Education, Inc.

She has served on succession, governing, and compensation committees in her board service, including Board of Directors of the Council for Higher Education Accreditation (CHEA) and co-Chair of CHEA's Commission on Quality Assurance and Alternative Higher Education. She is also a Trustee with the German Marshall Fund of the United States; a partner with the Houston-based Allen Austin Global Executive Leadership Firm; a member of the Atlantic Council; and an advisor for the Canadian Defense College Foundation.

Rondeau holds a bachelor's degree in history and social science from Eisenhower College, a master's degree in comparative government from Georgetown University, and a doctorate in education from Northern Illinois University, and has attended several senior executive training and education courses.

LtGen Keith J. Stalder, USMC (Ret.)
Former Commanding General, U.S. Marine Corps Forces, Pacific

LtGen Stalder was the senior Marine Corps Military Representative to the U.S. Pacific Command for operations in the Pacific, including Japan, China, North and South Korea, Guam, and Okinawa. The largest field command in the Marine Corps, it encompassed the operational forces of I and III Marine Expeditionary Forces. He directed and supervised Marine Corps bases in Japan, Okinawa, Korea, and the western United States, with 90,000 people, 500 aircraft, and 17 bases and stations. Previous high-level assignments include command of II Marine Expeditionary Force, Marine Corps Training and Education Command, 3rd Marine Aircraft Wing, and 1st Marine Expeditionary Brigade. LtGen Stalder is a Senior Fellow at CNA.

He holds an undergraduate and graduate degree in aeronautics from Embry-Riddle Aeronautical University.

Rear Admiral David W. Titley, USN (Ret.)
Former Oceanographer and Navigator of the Navy

Rear Admiral David Titley retired from the Navy in 2012. Dr. Titley is now a senior scientist in the Department of Meteorology at Penn State University. He is also the founding director of Penn State's Center for Solutions to Weather and Climate Risk. Dr. Titley served as a naval officer for thirty-two years, rising to the rank of rear admiral; his career included duties as Oceanographer and Navigator of the Navy. In 2009, he initiated and led the U.S. Navy Task Force on Climate Change. Titley holds a bachelor of science in meteorology from Penn State. From the Naval Postgraduate School, he earned a master of science in meteorology and physical oceanography, and a Ph.D. in meteorology. He was elected a fellow of the American Meteorological Society in 2009.

General Charles F. "Chuck" Wald, USAF (Ret.)
Former Deputy Commander, Headquarters U.S. European Command (EUCOM)

General Wald retired from the U.S. Air Force as a four-star general after serving over 35 years in the U.S. military as a command pilot with more than 3,600 flying hours and 430 combat hours. In his last position, he served as deputy commander of U.S. European Command (EUCOM) from 2002 until his retirement from the U.S. Air Force in July 2006. In that role, he was responsible for U.S. forces operating across 91 countries in Europe, Africa, Russia, parts of Asia, the Middle East, and most of the Atlantic Ocean. During his command, he developed the European Command Strategic Plan that included energy assurance and sustainment for the EUCOM area of responsibility.

General Wald commanded the 31st Fighter Wing at Aviano Air Base, Italy, where on August 30, 1995, he led one of the wing's initial strike packages against the ammunition depot at Pale, Bosnia-Herzegovina. From 1999 to 2001, he commanded the 9th Air Force and U.S. Central Command Air Forces at Shaw Air Force Base in South Carolina. In September 2001, as the Supporting Commander, General Wald led the development of the coalition air campaign in Operation Enduring Freedom, including the idea of embedding tactical air control parties in ground Special Operations Forces against Taliban forces in Afghanistan.

General Wald is a command pilot with more than 3,600 flying hours, including more than 430 combat hours over Vietnam, Cambodia, Laos, Iraq, and Bosnia. The General earned his commission through the Air Force ROTC program in 1971. He earned his master's degree in international relations from Troy University and received a bachelor of arts degree in pre-law from North Dakota State University.
He currently serves as Vice Chairman, Federal Practice Senior Advisor at Deloitte Services, LP.

Lieutenant General Richard C. Zilmer, USMC (Ret.)
Former Deputy Commandant for Manpower and Reserve Affairs, Headquarters Marine Corps, and Former Commanding General of Multi-National Force–West, Al Anbar Province, Iraq

Lieutenant General Richard Zilmer retired from active duty in January 2011 following over 36 years of commissioned service. During his military career, Zilmer served in a variety of operational and staff assignments throughout the United States, the United Kingdom, Germany, and Japan. His operational commands consisted of Commanding Officer, First Battalion, First Marines; Commanding Officer, 15th Marine Expeditionary Unit; Commanding General, Multi-National Force–West (Al Anbar Province, Iraq); and Commanding General, III Marine Expeditionary Force, Okinawa, Japan. Zilmer served combat tours during peacekeeping operations in Lebanon, Operation Desert Storm, and Operation Iraqi Freedom. Zilmer's staff assignments included multiple Washington DC tours at Headquarters Marine Corps and Deputy J-3 for Operations at EUCOM. His final assignment was Deputy Commandant for Manpower and Reserve Affairs, Headquarters Marine Corps.

Lieutenant General Zilmer graduated with a bachelor's degree in secondary education from Kutztown University in 1974, and holds a master of arts degree in national security and strategic studies from the College of Naval Warfare.

References

[1] Tett, Gillian. "Will Cyber Attacks Switch Off the Lights?" *FT Magazine*, April 24, 2015, http://www.ft.com/cms/s/0/ed59e166-e92d-11e4-a71a-00144feab7de.html.

[2] Klinger, C., O. Landeg, and V. Murray. "Power Outages, Extreme Events and Health: A Systematic Review of the Literature from 2011–2012." *PLoS Currents* 6, 1 (Jan. 2, 2014), doi: 10.1371/currents.dis.04eb1dc5e73dd1377e05a10e9edde673.

[3] U.S. Department of Energy/Infrastructure Security and Energy Restoration Office of Electricity Delivery and Energy Reliability. *Large Power Transformers and the U.S. Electric Grid.* June 2012. http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf

[4] Parfomak, Paul W. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations.* Congressional Research Service Report R43604, June 17, 2014, http://fas.org/sgp/crs/homesec/R43604.pdf.

[5] National Research Council. *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop.* National Academies Press, 2013, http://www.nap.edu/download.php?record_id=18535.

[6] Smith, Rebecca. "U.S. Risks National Blackout From Small-Scale Attack: Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage." *The Wall Street Journal,* March 12, 2014, http://www.wsj.com/articles/SB10001424052702304020104579433670284061220.

[7] U.S. Department of Energy/Office of the Inspector General. *Inspection Report: Review of Controls for Protecting Nonpublic Information at the Federal Energy Regulatory Commission.* Report DOE/IG-0933, January 2015, http://www.energy.gov/sites/prod/files/2015/02/f19/DOE-IG-0933.pdf.

[8] National Research Council. *Terrorism and the Electric Power Delivery System.* National Academies Press, 2012, http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system.

[9] CNA Military Advisory Board. *Powering America's Defense: Energy and the Risks to National Security,* May 2009, https://www.cna.org/sites/default/files/Powering%20Americas%20Defense.pdf.

[10] California State Senate. "Analysis of Senate Bill 699 as amended August 22, 2015," August 27, 2015, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml;jsessionid=a542d9f744a517b9aa5e97d45056.

[11] Smith, Rebecca. "Assault on California Power Station Raises Alarm on Potential for Terrorism." *The Wall Street Journal,* February 5, 2014, http://www.wsj.com/articles/SB10001424052702304851104579359141941621778.

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

[13] U.S. Department of Energy/Office of Electricity Delivery and Energy Delivery. *Energy Delivery Systems Cybersecurity*. Accessed July 2015. http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity.

[14] Executive Office of the President. *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. August 2013, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[15] Lipton, Eric, and Clifford Krauss. "Military to Deliver Fuel to Storm-Ravaged Region." *The New York Times,* November 2, 2012, http://www.nytimes.com/2012/11/03/business/military-to-deliver-fuel-to-storm-region.html?pagewanted=all&_r=0.

[16] Summary. *Severe Space Weather Events–Understanding Societal and Economic Impacts: A Workshop Report*. Washington, DC: The National Academies Press, 2008. http://www.nap.edu/openbook.php?record_id=12507&page=1.

[17] WUSA 9 News. "Equipment failure causes power outage in DC, Md." WUSA 9 News Online, April 7, 2015, http://www.wusa9.com/story/news/local/2015/04/07/power-outage/25411283/.

[18] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Report of the Defense Science Board Task Force on DOD Energy Strategy*. February 2008, http://www.acq.osd.mil/dsb/reports/ADA477619.pdf.

[19] American Society of Civil Engineers. *Failure to Act: The Economic Impact of Current Investment Trends in Electricity Infrastructure.* ASCE, 2011, http://www.asce.org/uploadedFiles/Issues_and_Advocacy/Our_Initiatives/Infrastructure/Content_Pieces/failure-to-act-electricity-report.pdf.

[20] Solar Energy Industries Association. "Solar Energy Facts: 2014 Year in Review." December 17, 2014, http://www.seia.org/sites/default/files/Q4%202014%20SMI%20Fact%20Sheet.pdf.

[21] Director General, International Atomic Energy Agency. "Nuclear Technology Review 2013," GC(57)/INF/2 (July 22, 2013), https://www.iaea.org/sites/default/files/gc57inf-2_en.pdf.

[22] Sandia National Laboratories. "SPIDERS Microgrid project secures military installations." February 22, 2012, https://share.sandia.gov/news/resources/news_releases/spiders/.

[23] University of Texas. "The Role of Microgrids: A Perspective from the University of Texas at Austin," May 2015, http://www.utexas.edu/research/cem/smartgrid_images/The%20Role%20of%20Microgrids.pdf. (White paper provided by Gen. Ken Eickmann, U.S. Air Force (Ret.), Military Advisory Board member.)

[24] *Pecan Street Smart Grid Demonstration Program—Final Technology Performance Report*. Smartgrid.gov. February 2015, https://www.smartgrid.gov/document/pecan_street_smart_grid_demonstration_program_final_technology_performance_report.html.

[25] Wood, Elisa. "How 3 states are moving forward with micro-grids." GreenBiz.com. July 8, 2014, http://www.greenbiz.com/blog/2014/07/08/how-3-states-are-moving-forward-microgrids.

[26] Office of the Under Secretary of Defense (Installations and Environment).*Department of Defense Annual Energy Management Report: Fiscal Year 2013*. June 2014, http://www.acq.osd.mil/ie/energy/energymgmt_report.

[27] Marqusee, Jeffrey. "Microgrids and DOD Facilities." SERDP/ESTCP briefing. June 12, 2012, http://energy.gov/sites/prod/files/Presentation%20to%20the%20EAC%20-%20Microgrids%20and%20DoD%20Facilities%20-%20Jeffrey%20Marqusee.pdf.

www.cna.org/mab/assured-electrical

ANALYSIS & SOLUTIONS