DOUBLE ISSUE

CST & CBRNE SOURCE BOOK

SECURITY & BORDER PROTECTION

tacticaldefensemedia.com | Fall 2014

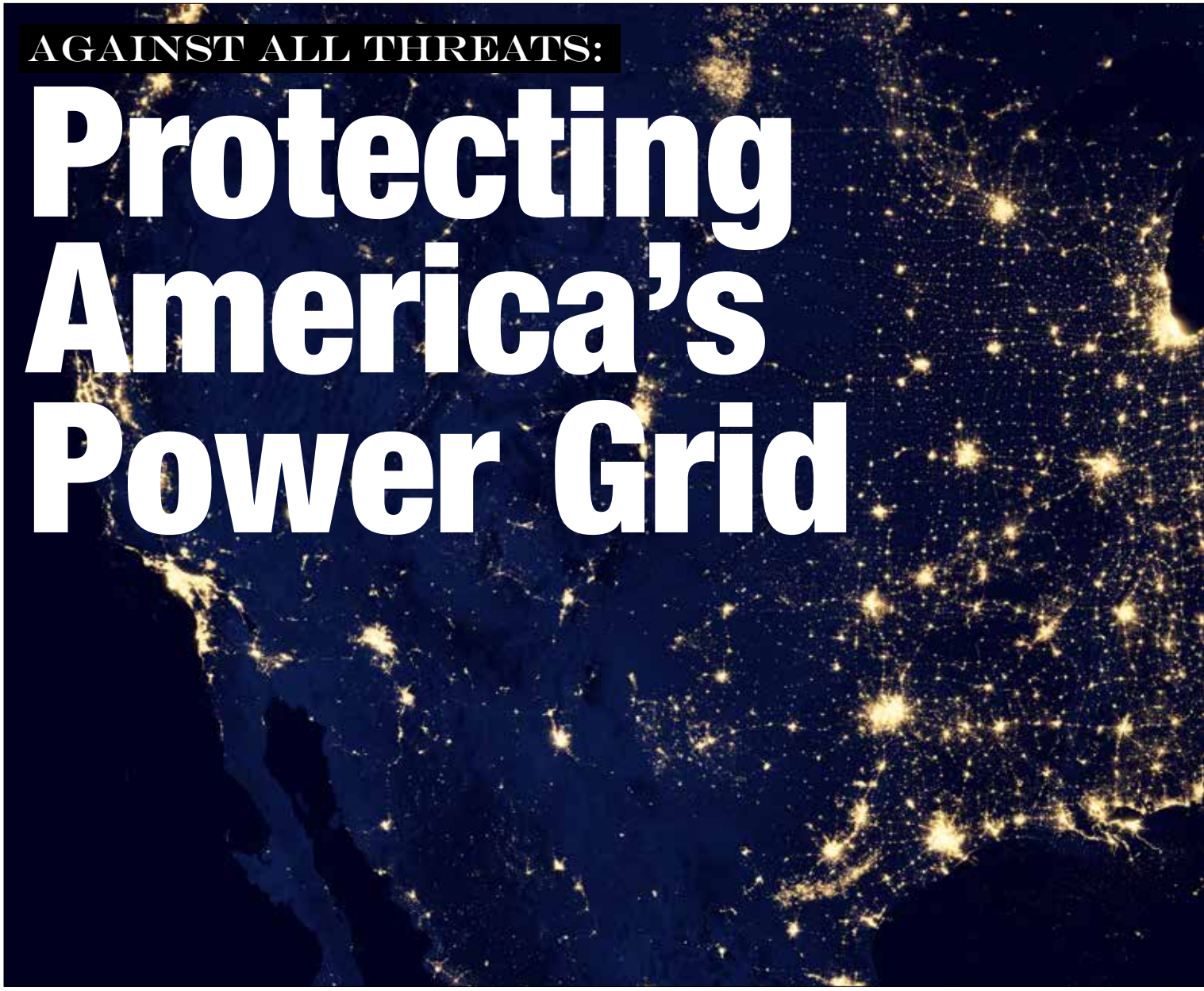
PROTECTING THE GRID
The Spectrum of Threats

COUNTERING NUCLEAR TERRORISM THROUGH DETECTION AND FORENSICS
Interview with Dr. Huban Gowadia, Domestic Nuclear Terror Office

Commander's Corner

BG Jonathan Ives
Deputy Commander
377th Theater Sustainment Command
Belle Chasse, LA

20th Support Command Training ■ Local Outlook: Yuma Sector ■ Mobile Surveillance ■ Bio-protection



AGAINST ALL THREATS:

Protecting America's Power Grid

S&BP asks experts about the best ways to protect electrical infrastructure from physical and cyber attacks, geomagnetic disturbances, an electromagnetic pulse, and radio frequency and microwave weapons.

By Steve Melito, TDM Contributing Correspondent

One day after the Boston Marathon Bombing, American soil was the site of a different type of attack. Operating under cover of darkness on 16 April 2013, unknown assailants disabled a piece of electrical infrastructure in one of the most populous parts of California. At the Metcalf transmission substation near Silicon Valley, attackers cut underground fiber optic cables, deactivating security and communications. Using high-powered rifles, they then began a 20-minute barrage on the substation's 17 transformers and cooling system. By the time police arrived, the marksmen had fled, leaving only spent casings without fingerprints.

Damage to the Pacific Gas and Electric facility forced the re-routing of electricity, and repairs took several months. Initially, the FBI dismissed claims that the incident was a terrorist attack, and Santa Clara County Sheriff Laurie Smith described it to local reporters as "sabotage." John Wellinghoff, who was then chairman of the Federal Energy Regulatory Commission (FERC), would later call the attack "the most significant incident of domestic terrorism involving the grid that has ever occurred."

A National Blackout?

As the federal agency charged with ensuring the reliability of the nation's power supply, FERC was featured in a 12 March 2014 article in the *Wall Street Journal* on the risks of a national blackout resulting from a small-scale attack. The story, which quoted Wellinghoff, revealed aspects of a FERC study that forecast the devastating effects of a coordinated attack on just nine of the country's 55,000 electrical-transmission substations. Several U.S. Senators joined industry trade groups in demanding an investigation into Wellinghoff's role in this disclosure, while other legislators responded by re-introducing

Satellite imagery of the U.S. at night underscores the nation's dependence on electricity. (NASA Earth Observatory, Robert Simmon)

the Grid Reliability and Infrastructure Defense (GRID) Act, which eventually died in committee.

The 2014 GRID Act echoed a May 2013 Congressional staff report called "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps." Published just a month after the physical attack at Metcalf, the report claimed that "the electric grid is the target of numerous and daily cyber-attacks." Most utilities comply with mandatory standards for cybersecurity, but have not yet implemented voluntary safety recommendations from the North American Electric Reliability Corporation (NERC), a non-profit international authority. "Physical damage by terrorists to large transformers," the report added, "could disrupt power to large regions of the country."

In seeking to provide additional regulatory authority to FERC, the 2014 GRID Act sought a stronger standards-making role for NERC. The proposed legislation also cited potential threats such as an electromagnetic pulse (EMP), geomagnetic disturbance, and radio frequency or microwave weapons. By producing a powerful electromagnetic disturbance, a man-made device such as a nuclear weapon or a natural event such as a geomagnetic storm could destroy or disable electronic equipment. The scope of the damage would depend on the nature and power of the weapon.

Many of us in the industry years ago always suspected a high-probability attack would be exactly what happened at Metcalf.

Although some national security analysts have warned that Iran or North Korea could cripple the power grid by detonating a nuclear weapon high above the U.S. heartland, other experts discount this threat because of its relatively low probability. Meanwhile, recent cyber attacks such as Dragonfly have hit grid operators, electricity generation firms, and energy industry equipment providers. As the computer security company Symantec reported on 30 June 2014, "Dragonfly bears the hallmarks of a state-sponsored operation," possibly from Russia, and "is well resourced, with a range of malware tools at its disposal."

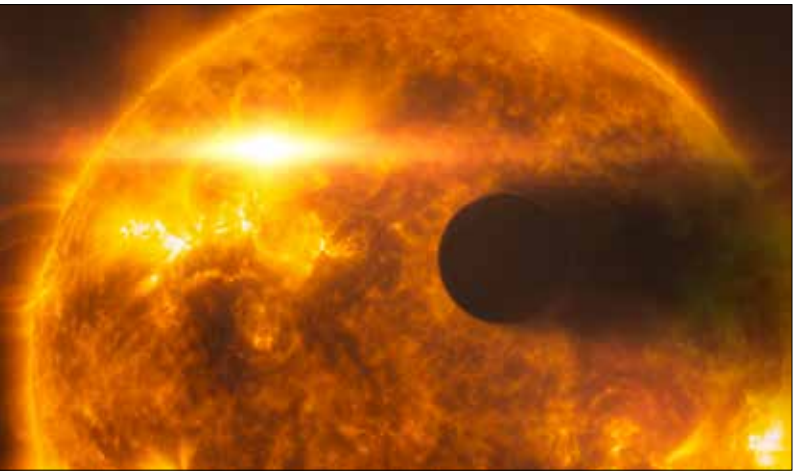
Physical and Cyber Attacks

For Chris Humphreys, director and CEO of the The Anfield Group, Inc., based in Austin, TX, new regulations won't necessarily help the electric power industry to address physical and cyber threats. Humphreys, who started his career at the Department of Homeland Security's National Infrastructure Coordination Center, explained to S&BP that the current regulatory approach is "an unsustainable model." His company, which provides security convergence and compliance strategy services to bulk electrical system asset owners, helps electrical utilities plan and prepare for a spectrum of threats.

Before starting The Anfield Group, Humphreys was the development lead at the United States Computer Emergency Response Team and the Critical Infrastructure Protection (CIP) Manager for the Defense Department's Counterintelligence Field Activity. A certified NERC Compliance Auditor, he also served as NERC CIP Program Manager at Texas Regional Entity, Inc., the FERC-approved Regional Entity for the Lone Star State. Humphreys said that federal regulators need to focus on "viable threats," including "real-world problems" such as the theft of copper wire from electrical substations.

The Metcalf attack may seem spectacular, but "many of us in the industry years ago always suspected a high-probability attack would be exactly what happened at Metcalf," Humphreys noted, adding that the rifle assault required "less effort than a coordinated cyber attack." That doesn't mean digital threats should be discounted, however. "I see cyber attacks as far more likely than physical [ones]," said Humphrey's colleague at The Anfield Group, Patrick C. Miller. "They are happening right now, and they can do it without setting foot on our soil—which has numerous advantages."

To strengthen grid security against physical and cyber attacks, regulators and the industry need to evolve. "There's still not a sense of proactively mitigating these attack methods within the industry," Humphreys said, "and regulation is completely reactive." He believes regulations need to feature a more "proactive" approach instead, but without "a shift to granularity" that is unsustainable for grid



Solar flares can cause geomagnetic storms that induce high current in power lines and result in the failure of transformers. (NASA, ESA, L. Calcada)

operators and asset owners. At a time when some utilities are still using email and spreadsheets to track compliance, automation will become essential for reporting.

Power industry executives may need to adjust their perspectives. "The compliance framework is a baseline," Humphreys contended, so complying with regulations doesn't necessarily mean that a utility or facility has taken all of the necessary security measures. By implementing "operational and security best practices" such as those outlined in NIST 800 series publications, however, the industry can chart a more sustainable path than "chasing compliance with the latest regulation," which in the case of cybersecurity especially, "tends to be a moving target." NIST 800 series publications are produced by the National Institute of Standards and Technology (NIST), and address not only computer security, but collaborative activities between industry and government.

By providing "a more focused set of regulations" instead of layers of new requirements, the CEO of The Anfield Group can envision consolidated standards that apply not just to the electrical power industry, but also to "multiple verticals such as oil and gas". By applying the NIST approach to risk management, for example, NERC's CIP V5 Program is already taking some steps in this direction.

Humphreys also pointed out that the formation of a separate, detailed set of physical security standards to complement current and future cyber standards is also possible. NERC is unlikely to mandate specific products, but may require technologies such as physical access control systems, monitors, closed circuit TV, physical penetration tests, access control, and badging control. The electric power industry could be required to complete more audits and third-party assessments, too. Finally, Humphreys noted, "enterprise-wide governance, risk, and compliance solutions" are critical to balancing operations and security with compliance.

EMP Attacks and Geomagnetic Storms

Michael A. Caruso, director of government and specialty business development for ETS-Lindgren Inc., is also working with industry leaders and following the legislation and regulations that could affect them. Although the GRID Act of 2014 went dark, Caruso sees a brighter future for H.R. 3410, the Critical Infrastructure Protection Act (CIPA), since it "shifts responsibility to the Department of Homeland Security (DHS)." Under CIPA, the Assistant Secretary of the DHS National Protection and Programs Directorate would include EMP events in national planning scenarios and educate CIP owners and operators about EMP threats.

Caruso has been advising power companies about EMP threats for several years, and recently worked with a large operations and data center that is the first such facility to be EMP-protected. ETS-Lindgren Inc., based in Cedar Park, TX, and a subsidiary of ESCO Technologies, is a leading provider of detection, measurement, and management technologies for electromagnetic energy. The company's Red Edge™ Pulse Protection line includes enclosures, doors, filters, and vents that are designed by professional engineers and independently certified by Little Mountain Test Facility, an Air Force Materiel Command laboratory dedicated to simulation testing of nuclear hardness, survivability, reliability, and electromagnetic compatibility of defense systems.

As Caruso explained to S&BP, power industry executives need to consider that there are two types of EMP attacks: intentional electromagnetic interference (IEMI) and high-altitude electromagnetic pulse (HEMP). Geomagnetic storms caused by solar flares are "different problems with different solutions," he said. EMP shielding can block the radiated effects, but the DC currents that are imposed on power lines must be treated separately. Protecting against geomagnetic storms alone can reduce—but will not block—the effects of an EMP attack. "The biggest challenge is in treating points of entry," such as doors, power lines, control lines, and fire alarms, he noted.

Caruso is concerned about all of these threats, but describes IEMI attacks as "medium probability and high impact." IEMI devices are relatively inexpensive and easy to construct, and can be vehicle-borne or hand-carried. Unlike the Metcalf incident, which lasted approximately 30 minutes, an IEMI attack is what Caruso termed "a drive-by event." Such an attack could happen so quickly, he told S&BP, that computer loggers could not register it. "Within 10 nanoseconds, it's over," he claimed.

Although a HEMP attack is less likely than an IEMI incident, the detonation of a nuclear weapon above 30 kilometers in the atmosphere could effect a wide area across the U.S. The detonation of a nuclear device at lower altitudes would produce an EMP pulse that's probably less intense, but still strong enough to induce fields that would cause electrical systems to fail in a more localized area. To mitigate potential HEMP effects, the U.S. military establishes an electrical perimeter around mission-critical facilities. Yet a large part of the energy infrastructure upon which the Defense Department depends is commercially-owned.

Hardening civilian facilities to the military standard is "overkill for industry," Caruso maintained, so ETS-Lindgren has "developed a more economical approach." Depending on what an operations center needs, a facility can choose Level 1 or Level 2 protection with the Red Edge line. Level 1 products protect critical assets such as transformers, but exclude generators and cooling systems. Level 2 products protect all of a facility's infrastructure and support continuous operations.

Ops centers are important, but they're not the only parts of the grid that require protection. "There's a need to protect the relays and switching operations at remote substations, too," Caruso noted. He also said that power companies need to install "neutral blocking devices" on high and medium voltage transformers.

Determining whether a facility needs to enclose units separately or install EMI-shielded rooms to protect every asset is part of ETS-Lindgren's consulting process.

Understandably, the electric power industry is concerned about costs. For a new operations center, Caruso estimated that EMP protection could account for as much as 20 percent of the construction total. In terms of total costs, including operations, that amount is significantly lower – typically six to seven percent. For industry executives then, it's essential to determine "what must stay live" and what can be "sacrificed." Medium and high voltage transformers are expensive to replace and require protection, whereas rooftop microwave communications links are lower-cost items, and spares can be warehoused off-site.

Retrofitting an existing facility also requires analysis. Older, wooden buildings can't attenuate signals from an IEMI device or HEMP attack. Concrete buildings with metal roofs provide some protection, and metal-clad buildings offer even more. By enhancing an existing structure with several small rooms or enclosures, utilities can contain costs. Utilities can also begin by protecting critical systems, and then upgrade to protect the entire facility. "There are things that can be done," Caruso stressed.

Small Grids, Big Changes

"If you're going to talk about protecting the grid," explained Jack Eisenhauer, president and CEO of Nexight Group LLC in Silver Spring, MD, "it needs to be in the context of how it's changing." For 35 years, Eisenhauer has led planning efforts in fields such as infrastructure protection and resilience, cyber security, and advanced energy technologies. Past projects include work on studies for the DHS National Infrastructure Advisory Council and the Advanced Grid Integration Division at the Department of Energy.

"Every sector is dependent upon the power grid," Eisenhauer told S&BP, "but the whole structure of the grid is changing in a fundamental way." These changes, he contended, are driven by new technologies, competition, and business models. Traditionally, the focus of the grid was maximum reliability built around centrally-controlled, base-load power generation. Today, a new class of power producers is emerging. This includes factories, universities, and even home owners who generate their own power, often with solar panels and other renewable sources.

Distributed power generation may represent the most significant transformation to the grid in decades. "New technologies that enable energy consumers to become energy producers and create micro grids," Eisenhauer explained, "are moving the U.S. towards a transitive energy model." These changes could force the loosening of constraints on the purchase and sale of electric power, which traditionally has been well-controlled. In an environment where individuals provide their own electricity, such as after a major power disruption, there are questions about how operators would manage the flow and "what the grid would look like," Eisenhauer said.

A broad portfolio of advanced grid technologies known as the "smart grid" is also changing the industry. An electricity supply network that uses digital communications technology to detect and react to local changes in usage, the smart grid can "greatly reduce outage times and speed recovery," Eisenhauer said. Yet the smart grid also includes "millions of new access points," so smart meters and even appliances such as refrigerators can represent points of cyber vulnerability.

Cyber attacks could darken control rooms like this at power generation plants. (phys.org)

To address potential digital threats, Eisenhauer envisions a future of smarter devices and greater coordination between government and utilities. The electrical power industry already monitors suspicious activity, he noted, and collaboration between the private and public sectors is increasing. For proponents of resiliency, what Eisenhauer described as "almost a self-healing grid" holds great appeal. "The very technologies that are the focus of concern," he explained, "are also increasing the resilience of the grid by enabling distributed generation; providing faster, more automated recovery; and laying the foundation for a more robust and dynamic electric grid overall."

No Time to Lose?

For some, the future of power grid security is now. For example, Virginia-based Dominion Resources plans to spend up $500 million to harden its facilities over the next seven years. In addition to installing physical barriers and EMP protection, the Mid-Atlantic region's largest electricity supplier is ordering additional spares and storing these assets off-site in secure areas. The company also plans to build a new Systems Operations Center to replace its 1980s-era facility.

On the West Coast, Southern California Edison has been working with the Defense Department and intelligence agencies to implement advanced cyber security technologies. The initiative is part of the Irvine Smart Grid Demonstration, a public-private partnership that includes SCE; University of California, Irvine's Advanced Power and Energy Program; and the Department of Energy.

Maine may lack the population of the Mid-Atlantic or Southern California, but the New England state is also a leader in grid security. On 11 June 2013, Maine passed LD 131, which requires the state's Public Utilities Commission to examine vulnerabilities in the electrical transmission infrastructure to an electromagnetic disturbance or geomagnetic disturbance. State lawmakers cited a moderate solar storm in March 1989 that caused a province-wide blackout in nearby Quebec.

The electric power industry faces a spectrum of threats, and experts may disagree about which are most likely—and likely the most devastating. Still, inaction is not an option. "If the power grid were taken off-line in the middle of winter and it caused people to suffer and die, that would galvanize the nation," said retired Admiral Mike McConnell, former Chief of U.S. National Intelligence, in a 2009 television interview. "I hope we don't get there." ■