Kites in the Night

Critical Infrastructure Protection Architectures in an Era of Improvisational Malignant Devices

Robert Spousta, Steve Chan
Sensemaking/PACOM Fellowship, based at Swansea University (SU)'s Network Science Research Center (NSRC),
spousta@mit.edu, stevechan@post.harvard.edu

Bob Griffin
General Manager and CEO i2 Group
IBM
Tucson, AZ
Griffinb@us.ibm.com

Kathleen Kiernan
Center for Homeland Defense and Security
Naval Postgraduate School
Monterey, CA
Dr.k2@comcast.net

***Abstract*—*This paper contextualizes the nature of threats to critical infrastructure, especially vulnerabilities within electric grid systems, and analyzes key considerations for the protection architecture of such systems. By exploring historical case studies, we demonstrate the potential for blind spots in infrastructure protection policy, which can leave electric grids vulnerable to a variety of threats, including improvisational malignant devices. These devices in turn have the potential to catalyze cascading failure scenarios within interdependent critical infrastructure systems, constituting "wicked problems"[1, 2] [1] of complexity that bear relevance to a variety of public and private institutions responsible for the provision of essential services.*

***Index Terms*—*Aluminum Foil Kite, Brittleness, Resilience, Big Data, Collaborative Big Data Analytics, Complex Systems, Critical Infrastructure Protection, Improvised Explosive Device, Improvisational Malignant Device, Nature-Inspired Engineering, Network Science, Sensemaking, Streisand Effect, Soft Bomb, Smart Electric Grids, Translational Biomimetics.*

I. Introduction

Critical infrastructure, and the electric grid system in particular, is a backbone of modern civilization. Both developed and underdeveloped societies around the world rely upon electricity to power a variety of devices upon which individuals and organizations have come to depend — from refrigerators to coffeemakers, from phones to phone systems, from tablets to high performance computing systems, and the entire Internet of Things (IOT)[3].[2] These and many other devices, in turn, facilitate communication, transportation, socialization, education, security, commerce, and seemingly endless forms of both recreation and work facilitation. However, how **brittle** is the digital physical ecosystem which powers this IOT? While vast resources are continually invested towards the research and development of smaller, faster, and smarter technological devices, the question remains as to whether a comparable investment is being made towards the research and development of protective measures for the backbone upon which all of these devices and capabilities are dependent. The grid's vulnerability has long been recognized[4], and events in the recent past such as the Northeast blackout in 2003[5, 6] demonstrate the negative impact of power disruptions[7]. However, while such developments have precipitated improvements to the grid[8], can we say that the system is truly resilient? If the condition of other pieces of the nation's critical infrastructure is any indicator of the state of the grid, then former Transportation Secretary Ray Lahood's characterization of the U.S. highway system as a "big pothole"[9] is indeed disconcerting. Lahood's assertion also begets the question of whether the architecture of our critical infrastructure protection (CIP) is evolving along a trajectory commensurate with other newly emerging technologies, or is our backbone of critical infrastructure becoming increasingly vulnerable?

Under normal operating conditions, the interconnected systems[10] that enable the mosaic of constituent critical infrastructures[11], such as the electric grid, to function properly are fairly subject to a complex web[12] of interrelated and constantly fluctuating variables[34][13].

[1] Design theorist Horst Rittel first described wicked problems in the context of social and policy planning, contrasting them with tame problems, for which an exhaustive formulation of relevant variables is attainable and definitive solutions are objectively verifiable. Wicked problems are comparatively more open-ended, defying a clear definition of boundaries and blurring lines of causation. Similarly, Warren Weaver, the prominent scientist, mathematician, and pioneer of machine translation, categorized problems into those of simplicity, disorganized complexity, and organized complexity. Problems of organized complexity comprise situations with a significant amount of variables and interrelationships, too diverse to reduce to a simple formula, yet not overly vast for statistical probability models to work effectively. Problems of such a nature comprise the focus of this paper.

[2] Coined by Kevin Ashton in 1999, the concept of an Internet of Things (IOT) developed largely out of work at MIT's Auto ID lab in developing radio frequency identification (RFID) in order to maintain a computerized inventory of physical objects. Today, IOT refers to the ubiquitous connectivity of billions of devices around the world facilitated by the Internet.

[3] The diverse nature of these variables is evident in the North American Electric Reliability Corporation (NERC)'s extensive catalogue of reliability standards for electricity delivery and Critical Infrastructure Protection (CIP) within the North American Bulk-Power System.

[4] The wide variety of information covered under the Protected Critical Infrastructure Information (PCII) Program further demonstrates the myriad of factors, which influence the safe operation of the grid.

Maintaining synchronization and stability between the nearly 15,000 energy generating facilities and across the hundreds of thousands of miles of transmission and distribution lines that make up the North American grid is no simple task for a system that operates at 60 cycles per second.[14] Even basic variables, like energy supply and consumer demand are influenced by a host of contributing factors, from the market price of petroleum, to the efficiency of air conditioning (AC) units and other home appliances. Moving beyond this steady state of complexity, natural weather events[15][5], seismic activity[16][6], and human-induced change can all have an even greater destabilizing impact upon the functioning of the grid, particularly amidst a disaster event. Understanding the overall vulnerability of the grid system requires a detailed exploration of each system component; both in the context of its interactions with the rest of the system, and with the surrounding environment in which the system resides. Such an exploration typically uncovers layers of increasing complexity and interrelation[17] that must be accounted for in the system's design. If strong winds knock down the power lines, then simply putting up stronger poles (even with plastiques) will not suffice; after all, what if termites infest the new pole? If terrorists threaten to sabotage a transmission substation, then will just building a fence around the substation suffice? What if they fly an **aluminum foil kite** over the fence? In contrast to the vast and highly interconnected North American grid system, we pay particular attention to the grid systems of the Hawaiian islands, which represents a somewhat unique case in light of its nature as a truly islanded (i.e. independent) system that is simultaneously home to strategically high-priority national security organizations[7] and subject to a variety of extreme environmental events.

As a cursory investigation of any major disaster will demonstrate, serious problems rarely arise in isolation from a solitary causal factor[18-20]. Rather, as the saying goes "when it rains it pours[8]," and the complex interaction of many contributing variables has the potential to compound and build up pressure to exert stress on multiple weak points across a system simultaneously, or in close succession, that can produce chain reactions of devastating effects, or cascading failures[21, 22], within a **brittle** (non-resilient) system. Thankfully, not every storm or service disruption inevitably results in catastrophe[23], but such failures do occur with sufficient regularity and devastating consequence that warrants investigation. Therefore, let us briefly explore the spectrum of cascading failures through two examples. At the lower end of the spectrum, suppose that severe weather conditions result in knocking out power within a service area containing a water treatment plant. Without power going to the water treatment plant, untreated sewage can flow into public waterways leaving beaches unsafe for tourism and/or other commercial activities, thereby compromising the economic vitality of the region[9] (Waikiki Beach, Honolulu, Oahu 2006). At the higher end of the spectrum, suppose an underwater earthquake triggers a tsunami that impacts the coast of a developed island nation, precipitating the meltdown of several nuclear reactors and one of the worst radiation leaks in the world's history[24][10] (i.e. 2011 Japan Tsunami and Fukushima Nuclear Accident).

While such examples are useful in illustrating the catastrophic potential of cascading failure, conducting forensic analysis of an extreme scale disaster, after the fact, is considerably easier than identifying the precipitating ingredients comprising the recipe of a perfect storm that has yet to come (e.g. an encore performance of the 1946 Aleutian Tsunami, which impacted the Hawaiian islands[25]). In this paper, we consider the vulnerability of the electric grid by contrasting it with historical examples of efforts to defend large, complex systems against destabilizing threats and introducing the concept of the **improvisational malignant device** (IMD) as but one example of how a relatively low level of sophistication can achieve high level disruptive impact. We argue that a reorientation of CIP posture is in order which accepts the assumption of breach as an inevitable reality and incorporates resilient design into the grid's foundational architecture. In addition, we offer insights from the analytical methodology of Sensemaking in an effort to integrate cross-disciplinary perspectives that have the potential to increase the resilience of critical infrastructure systems like the electric grid.

II. THE PROBLEM WITH HARDNESS: WHAT CAN WE LEARN FROM THE MAGINOT LINE, PROHIBITION, AND THE IMPROVISED EXPLOSIVE DEVICE?

While an effort to enhance CIP is laudable and certainly necessary, a critical assessment of any such effort is required to actually determine its costs, benefits, and shortcomings. In

[5] The recently released National Climate Assessment from the Obama Administration's Global Change Research Program asserts that global climate changes are under way, resulting in increasingly severe weather events that will continue to occur with greater frequency, inflicting more damage and causing more loss of life.

[6] On October 15, 2006, earthquakes on Oahu caused mercury gauges in the Hawaiian Electric Company's electricity generators to register false positives for low fluid levels, resulting in a system-wide shutdown and a day-long blackout affecting 291,000 customers on the island of Oahu.

[7] Most notably, the U.S. Pacific Command (PACOM), which is responsible for planning and execution of all U.S. military activities in the Pacific Rim. PACOM's ability to operate reliably is particularly important in light of the U.S. pivot or rebalance toward security in the Asia-Pacific region, as enunciated in guidance documents like the 2012 "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense".

[8] Based on the epigram attributed to U.S. Air Force engineer Captain Edward Murphy that whatever can go wrong will go wrong, this quote is widely known as Zymurgy's seventh exception to Murphy's Laws. Zymurgy is also credited with the law of evolving system dynamics that once you open a can of worms, the only way to re-can them is to use a larger can.

[9] Many similar scenarios have occurred throughout the Hawaiian Islands, for example, in May 2014 the Department of Health issued a brown water advisory for the public to stay out of Lake Wilson in the Wahiawa region of Oahu due to a power failure that led to raw sewage entering the lake. Around the same time, the beaches of Kalapaki Bay on Kauai were closed because 500,000 gallons of raw sewage were released as a result of a power failure at the Lihue Wastewater treatment plant. Finally, a December 2003 power failure at Honolulu's Hart Street pumping station led to the release of nearly 5 million gallons of raw sewage spill into Honolulu Harbor, Nu'uanu Stream and Kapalama Canal.

[10] For additional details on the 2011 Japan earthquake, tsunami, and subsequent nuclear reactor meltdown, please consult reference [13].

discussing CIP, a logical starting point is to delineate key characteristics of the system and a general outlook or defense posture for safeguarding the system's operation. Is the grid nothing more than a rigid or static set of nodes and edges around which a wall is to be built for security, or is it more comparable to a flexible and adaptive organism that has the ability to take corrective action in the event of service disruption, like a bee colony reorganizing task distribution in response to changing conditions in and around the hive? Indeed, there is a balance to be struck between protecting individual physical assets at the component level, and instilling resilience through operational dynamics at the system-level[26]. Achieving a common understanding of how the grid is to be conceptualized is fundamental to developing more advanced means for its protection. In other words, do we architect CIP to be hard on the outside and focus inward, or do we start with a rugged interior that faces outward? Furthermore, are there other more viable concepts in the rapidly expanding realm of nature-inspired engineering[27][11] (e.g. translational biomimetics[12]) that could enhance the resilience of the grid?

With regards to CIP, the predominating trend tends to be towards so-called "hardening"[28], or adopting externally-focused measures to make individuals components of the system more impermeable or resistant to failure. Examples include building fences or walls around transmission substations, sheathing power lines with thicker protective material (or placing them underground), and fortifying generation and transmission facilities in order to withstand more extreme weather or seismic events[29].

While such measures do increase the grid's resilience against commonly occurring or easily predictable destabilizing events, they also bear similarity to the Maginot Line constructed by the French in the wake of the devastating trench warfare of the First World War[30]. Composed of a series of defensive fortifications, the Line was engineered to be a state-of-the-art security measure, replete with amenities, such as air-conditioned living quarters and an underground railway network[31]. Yet, for all the resources devoted to its construction, the Maginot Line was ineffective against the Blitzkrieg, whereby Nazi Panzer divisions maneuvered around the Line through the Ardennes Forest. The Allied defense strategy falsely assumed the Line guaranteed against any German invasion through France, and so the preponderance of defense forces prepared for an attack from the North through Belgium[32]. This overly simplistic threat assessment led to a crucial strategic miscalculation, leaving the French with minimal adaptive capability to mount an alternative defense to the German advance, thus securing their defeat in the early stages of the Second World War.

Similarly, hardening critical components of the electric grid with external protective measures like undergrounding, barbed wire, or reinforced concrete are effective in strengthening the shell surrounding the system. But, is the system itself more resilient? While a fence may dissuade a would-be saboteur from simply walking into a transmission substation, it does not prevent him from flying an **aluminum foil kite** over the fence in order to short out the transmission and distribution lines. Such measures cost money to implement[33] and necessitate even more money to re-deploy as the terrain and circumstances change. Hardening measures are undoubtedly effective against the most likely or easily predicted destabilizing events (e.g. seasonal storms, unsophisticated vandals, etc.), but what about those more extreme events that are more difficult to predict, and which, although rare in occurrence, may yield devastating impact (e.g. Superstorms, high-magnitude seismic events, competent and determined terrorists, etc.)[34]? While hardening critical infrastructure is useful for providing some added system security, it is not adaptable, and may actually introduce new weakness as the system trades responsiveness and flexibility for rigidity. Resilient structures are designed to flex; rigid structures are brittle and will fracture. In addition, external hardness measures may serve as markers, thus helping would-be saboteurs to identify critical nodes as potential targets for malicious action, similar to a phenomenon observed in cyberspace dubbed the Streisand Effect[13].

As the case of the Maginot Line suggests, no single defensive paradigm can definitively protect against all conceivable destabilizing forces, including natural disaster or human aggression. Indeed, it may actually be impossible to definitively defend against even a single destabilizing force. In order to explore this point further, let us consider the example of alcohol prohibition in the United States from 1920-1933 and what then-President Herbert Hoover termed the "Noble Experiment.[35]"

Prohibition was intended to rid the country of the deleterious effects of alcoholism, by outlawing the production and sale of alcohol[36]. Putting all judgment of such an experiment's nobility aside, what is clear about Prohibition is that it cost well over $150 billion, ultimately led to the

[11] Nature-inspired engineering refers to the adaptation of naturally occurring phenomenon for human applications, known more formally as translational biomimetics or biomimicry.

[12] Leveraging the autonomic nervous system as a model for sensory capability within the grid is one example that is addressed later in this paper. Other possibilities for further exploration include adapting the dentricle (the V-shaped structures that make up the rough skin of a shark) pattern formation in shark skin to build greater resistance to bio-fouling on exterior grid facilities (i.e. transmission line coating), leveraging spider silk's incredible tensile strength to construct more resilient transmission and distribution lines, or translating the chameleon's color-changing ability into flexible response capability for managing surges and service disruptions across the grid.

[13] Named for the famous singer who sued the California Coastal Records Project for publishing a picture of her Malibu mansion; online interest in the picture grew exponentially after news of the lawsuit spread. Similar to the concept of blowback, the **Streisand Effect** refers to an instance where efforts to suppress or safeguard information have the reverse outcome of drawing greater attention. An example of this effect is the case of the Massachusetts Bay Transportation Authority (MBTA)'s attempt to prevent MIT students from presenting findings from their research showing that the MBTA Charlie Card automated fare system was susceptible to being hacked. By seeking an injunction against the students, MBTA unwittingly precipitated the spread of information about the system vulnerability, as the students' research was accessed from the court's public website, then more widely disseminated.

increased consumption of hard liquor over wine and beer[14], and expanded the operations of modern organized crime and the black market in the United States[37][15]. While Prohibition developed from a desire to defend American citizens against their own self-destructive tendency to consume alcohol, the difficulty associated with implementing such a program is a lesson on the average citizen's propensity for creativity in circumvention and public policy's vulnerability to blind spots. Although the production and sale of alcohol was prohibited, organizations and individuals developed ingenious strategies to continue consuming the substance. Career criminals who were already making a living from illegal activities, such as prostitution and gambling, simply expanded their scope of operations to include bootlegging, or transporting and selling illegally produced alcohol. Al Capone's operation in Chicago is a well-known example of how enterprising gangsters developed sophisticated and expansive systems in order to facilitate the manufacture and sale of contraband liquor[38]. Capone's operation consisted of a vast human network of alcohol producers, speakeasy operators, complicit law enforcement officials, and politicians, as well as a complementary physical infrastructure of clandestine production and supply chain facilities, including a large network of underground tunnels linking distribution points.

However, this was not an era controlled solely by organized criminals; Prohibition also catalyzed many otherwise law-abiding citizens into subversive action in developing inventive ways to secretly produce and sell alcohol. Anecdotes abound related to the systems devised for underground alcohol distribution, from the barn in Massachusetts where for a five-cent entry fee, visitors could marvel at a striped pig and quench their thirst with complimentary alcoholic refreshments, to moonshine smugglers' experimentation with a variety of methods for transporting their product, including refilling and packaging emptied eggshells and constructing hidden compartments in baby strollers. Previously unreligious individuals sought to be ordained as rabbis and priests, as these high offices were granted exceptions to possess alcohol for religious ceremonies. While doctors were permitted continued access to alcohol for medicinal purposes, it is clear that such privileged access was abused in order to imbibe alcohol for the purpose of intoxication, as is evidenced by the case of Alcoholics Anonymous co-founder Dr. Bob[39]. Indeed, the complicity of doctors, police officers and other public servants in the underground liquor trade during the Prohibition era presents an interesting parallel to the insider threats, which confronts CIP today, in that the very individuals entrusted to defend public safety are uniquely positioned to compromise it. Moral considerations aside, the outcome of Prohibition demonstrates an important aspect of human nature that is relevant to the protection of the electric grid; given sufficient resources and motivation, an individual will find ways to achieve any desired end, regardless of the legal or physical barriers erected to prevent that end.

This same fact is further evidenced by the more recent example of the improvised explosive device (IED). Following the invasion of Iraq in 2003, insurgents faced an allied force that was superior in training, organization, and equipment. In response, insurgents resorted to the widespread use of IEDs as one of their few strategic advantages; a destructive force that was relatively simple to produce and hard for the adversary to detect, or prevent against[40]. More than a decade later, with $20 billion spent[41][16], the efforts of the Joint IED Defeat Organization (JIEDDO) and its partner agencies represent the largest publicly-funded wartime research and development program since the Manhattan Project's development of the atomic bomb during the Second World War. Indeed, JIEDDO's work has certainly saved many lives, improved our understanding of the threats posed by IEDs, and enhanced the ability of the national security apparatus to cope with the adversary's primary weapon of choice. However, given the complex nature of the threat, the U.S. and its allies are unable to prevent IED attacks, and instead focus efforts on minimizing the devices' effectiveness[42]. There is no singular solution to the problem of IEDs, and so a variety of methods have been developed to mitigate their negative impact, including tracking the production, sale, and movement of IED precursor materials[43], such as calcium ammonium nitrate (CAN), so as to disrupt the manufacture of devices, identifying the techniques and signatures of known IED producers, and developing methods for detecting and clearing planted devices[44]. But, this does not definitively prevent the production and employment of IEDs, unless the US counter-IED strategy moving forward is to strictly acquire all available fertilizer worldwide in the hopes of preventing its further distribution. On the contrary, JIEDDO has, unintentionally through its successes, driven adversaries to evolve increasingly sophisticated tactics, techniques, and procedures, thereby incurring ever greater costs in the form of human life and national resources[45]. As adversaries continue to adopt more advanced methods, JIEDDO and its partner organizations must work continuously to adapt their approach to counteracting the destructive impact of IEDs. Meanwhile, events like the Boston Marathon bombing in 2013[46] demonstrate that IEDs are not a distant threat limited to nations like Iraq and Afghanistan, but rather are a ubiquitous and persistent destabilizing global menace with no single solution. JIEDDO has adopted a mixed-methods approach of simultaneously pursuing the human network of IED

[14] In light of its higher alcohol content, liquor could deliver the same effects in smaller, more concealable quantities.

[15] Legislated January 19, 1920 as the Volstead Act, Herbert Hoover termed Prohibition "the Noble Experiment" for its intended effect of ridding the nation of the deleterious effects of alcoholism by prohibiting the manufacture and sale of alcoholic beverages. Over the next nine years, the U.S. Government spent $301 million enforcing the law, and suffered an estimated eleven billion dollar loss in untaxed (i.e. illegal) alcohol sales at the hands of organized crime syndicates, such as those lead by Al Capone. Adjusting for inflation via the U.S. Bureau of Labor and Statistics' CPI calculator [http://www.bls.gov/cpi/cpicalc.htm], Prohibition's final price tag rings in at nearly $155 billion in 2014 buying power.

[16] As noted in [37], between FY06-FY11 Appropriations for JIEDDO totaled $18B; subsequent appropriations have included $2.4 billion in the FY12 Consolidated Appropriations Act, Public Law (P.L.) 112-74; $1.6 billion in the FY13 Consolidated and Further Continuing Appropriations Act (P.L. 113-6); and $879 million in the FY14 Consolidated Appropriations Act (P.L. 113-76), for total of $22.879 billion.

producers, coping with technical aspects of the device, and preparing personnel with training and education[47]. Likewise, enhancing the resilience of the electric grid requires a mixed-methods approach that simultaneously strengthens external components of the system against routine disruptions, while also enabling the interior of the system to cope with extreme events.

As these historical examples demonstrate, implementing absolute defensive or preventive measures is fraught with difficulty, particularly when such measures are rigid, or inflexible. Similar to the shortcomings of the Maginot Line and alcohol prohibition, efforts to harden the electric grid are compromised by an underlying specious assumption that all threats to a system's stable functioning can be identified and mitigated against effectively. This assumption ignores the overwhelming body of evidence that circumstances inexorably change, threats constantly evolve, the unlikely does occur, and that a static defense which proves effective at a singular moment will not remain effective in perpetuity. As with the struggle to counter IEDs, we must accept that destabilizing events will inevitably challenge the normal functioning of the grid, and therefore a variety of measures are required to enhance its resilience, including the ability to adapt. In short, there are no easy or definitively permanent answers to complex problems, and any earnest attempt to secure critical infrastructure systems like the grid must incorporate adaptive capabilities. In order to highlight this need for adaptation, let us consider the nature of human threats to a stable electric grid.

III. WHAT GOES AROUND COMES AROUND: GULF WAR ONE AND THE GENESIS OF THE IMPROVISATIONAL MALIGNANT DEVICE

While a far cry from the tranquil shores of Waikiki, a legitimate threat to the stability of Hawaii's critical infrastructure has its origins in the deserts of Iraq. In preparing for Operation Desert Storm, U.S. military planners determined that Saddam Hussein's national level air-defense system, including the supporting computers and ground-based radar, was a key center of gravity for decisive operations at the outset of the war. But, in order to disable Iraq's air-defense capability, the U.S. first had to disable the electric grid[48]. Since World War II, electric grid systems had been recognized as strategically significant targets, and during the Korean and Vietnam Wars, the bombing of electricity generation and transmission facilities indeed yielded considerable operational impact[49]. However, by the time of the Persian Gulf War, the legality of destroying civilian targets like the electric grid was under scrutiny[50], and military planners were compelled to seek methods of disabling the grid without destroying facilities outright. Therefore, in addition to the precision-guided munitions deployed to cripple Iraq's grid, the military also air dropped graphite wire and metal shards over Iraqi open-air transformer switching yards[51, 52][17]. Similar "soft bombs" were also deployed by U.S.-led North Atlantic Treaty Organization (NATO) forces over Kosovo in 1999 in response to genocidal violence perpetrated by Serbian armed forces[53] in the region. While they constituted vital components of strategic military air campaigns, these weapons were little more than metal wire and small graphite filaments dispersed from warheads[54], which established short circuits between critical pieces of transmission equipment, creating high-energy arcs and power surges that ultimately blacked out the targeted grid systems. Such a technique presents a strikingly profound irony; one of the most complex and costly pieces of a country's infrastructure can be compromised with relative ease by employing one of the most inexpensive and readily available materials at any supermarket or hardware store. Over two decades later, electric grids across the United States remain vulnerable to the same commodity.

While the soft bombs deployed over Iraq and Kosovo were delivered by rockets, it is not hard to conceive of a cost-efficient delivery method for the IMD. First, let us consider the fact that a box of 75 square feet of Reynolds Wrap aluminum foil is a viable dispersion component, ideal for its conductivity and availability (i.e. it costs about five dollars and can be purchased at nearly any supermarket, convenience store, or online). In addition, a variety of unmanned aerial vehicles (UAV)s are available at physical and online retailers like Brookstone, from the very practical *QFO Quad Fighter Mini Remote Controlled Gaming Drone* (which boasts six axis maneuvering with automatic stabilization and 2.4 GHz digital wireless with remote pairing capability for only $100), to Apple's top-of-the-line *Parrot AR.Drone 2.0 Power Edition Quadricopter* (which can be piloted from an iPhone for $369.95). Such devices could be piloted onto open air transformer switching yards with enough aluminum foil or mylar to generate similar short circuits as those achieved by smart bombs[55] . Although the use of UAVs or drones for malicious purposes has been recognized, policy makers and regulatory agencies are challenged to keep pace with the rapidly evolving technology[56], thus making such devices ideal for employment as IMD components.

Given the simplicity with which it can be acquired and deployed to yield destabilizing or disruptive impact, we categorize such a threat as an improvisational malignant device (IMD). In contrast to the destructive capacity of the IED, an IMD is characterized by its capacity to disturb or destabilize a system's normal functioning without completely destroying the system. The hallmark of the IMD is its ability to yield highly impactful results at a relatively low level of sophistication and cost.

While natural disasters remain the most common cause of energy disruption, malicious activity targeting critical infrastructure like the grid is clearly on the rise[57]. For example, unidentified gunmen successfully disabled a San

[17] Conceived largely by Colonel John Warden III and the Pentagon Air Staff's Project Checkmate, Instant Thunder was the air component of Operation Desert Storm, developed at the request of then U.S. Central Command (CENTCOM) Commander General Norman Schwarzkopf. Modeled after Operation El Dorado, the 1986 air raid on Libya, Phase 2 of Instant Thunder was aimed at disabling Iraqi civilian infrastructure, primarily the electric grid, by air-dropping metallic debris onto transformers, thus shorting out the electric grid.

Jose substation more than a year ago with no suspects identified or motives understood as pertains to what the Chairman of the Federal Energy Regulatory Commission (FERC) called the "most significant incident of domestic terrorism involving the grid that has ever occurred"[58][18]. Similar malicious acts in 2005 in Florida[59] and 2013 in Arkansas[60] demonstrate that individuals are willing and able to carry out attacks on the grid. Indeed, the interconnected nature of the grid makes it vulnerable to targeted attack[61]. This is particularly true of the critical components that make up the grid, such as the approximately 2,000 high voltage (HV) transformers, which comprise only 3% of transformers in the North American grid system, yet convey 60-70% of the grid's energy[62]. In light of these vulnerabilities, what steps are being taken or should be taken to enhance the grid's resilience?

IV. TOWARDS A MORE RESILIENT GRID

Bearing in mind these historical examples and hypothetical scenarios, we now turn back to a consideration of the current state of the electric grid(s) in the United States, and Hawaii in particular. If the U.S. military was able to cripple one of Saddam Hussein's most critical national assets with a bit of wire and filament, what is preventing a motivated individual from blacking out the island of Oahu with a skillfully piloted Mylar kite, or UAV? While an IMD deployment like this would certainly constitute a significant incident of domestic terrorism, it is no leap of the imagination to see that such an act would not require an extensive amount of resources or expertise. In order to arrive at this appreciation of the grid's vulnerability, we have employed a variety of historical and systematic lenses, each of which illuminate unique and critical points about the nature of the grid as a complex system, and the inherent challenges of safeguarding such a system against destabilizing elements. Like Benjamin Franklin's bifocals, this mixed lens brings critical insights into focus, raising important questions about the nature of infrastructure protection.

Rather than assuming that attacks on the grid can be comprehensively prevented, it is clear that we can safely assume that attacks on the grid and other destabilizing events will inevitably occur. If preventing attack is no longer the objective, how does the protection architecture take shape? In addition to identifying what individual points within the grid system are most likely to be targeted due to their essential role in the system's overall operation, we must also look at how every component in the system interacts and can be leveraged to enhance the system's collective resilience. Therefore, hardening the grid is but one step in the pursuit of a defense-in-depth paradigm[63][19], whereby would-be saboteurs are forced to expend greater effort in order to achieve destructive effects against fortified targets within a system that is designed to operate effectively in response to destabilizing events. Incorporating this resilience into the fabric of the grid system's design is not straight forward and will require thoughtful innovation and deliberate compromise with other system dimensions.

In addition to the necessity of increasing the grid's resilience and reliability, we cannot ignore the imperative for the grid to operate more efficiently by incorporating renewable energy sources[64]. However, renewable sources like solar and wind energy are intermittent, and thus inherently less stable than conventional sources like fossil fuel. The sun does not always shine, and the wind does not always blow, but power must always flow across the grid nevertheless[65]. These competing demands indeed represent a paradox, and so a balance between them must be deliberately and consciously struck. In this vein, innovations like Enphase Energy's microinverter allows for more effective and stable integration of solar or photovoltaic (PV) energy generation into the grid[66]. But, in Hawaii and elsewhere in the U.S., integrated PV power generation represents a fractional share of the overall energy portfolio, such that the advent of microinverters does not represent a sea-change improvement in grid operations. Similarly, advancements like Dominion Voltage Inc's (DVI) Edge platform, which leverages an advanced metering infrastructure (AMI) or smart meters for voltage conservation and distribution automation will no doubt be a mainstay of the smart grid moving forward[67]. However, Edge and other similar metering tools are consumption-centric and do not directly address either issues of system stability or the prevention and remediation of service disruption. In addition, the arrival of microinverters and AMI introduces new vulnerabilities into the grid due to their interconnected nature and susceptibility to being hacked or tampered with[68]. Such innovations are a double-edged sword; while microinverters and smart meters enhance the sophistication with which the grid operates, they also add layers of complexity and introduce new attack vectors for malicious actors.

There is no single panacea or silver bullet solution for increasing the grid's resilience. Just as there are a wide variety of potential threats to the grid's stable functioning, there are numerous potential enhancements to ruggedize its operation. Certainly, a logical starting point is the current endeavor to remove the aging elements of the system[20], which are most prone to failure (i.e. fossil-fuel dependent generating equipment[69]) in favor of modern components that are capable of serving the same function more reliably and at a

[18] On the night of April 16, 2013 in Santa Clara County, CA, a team of as-yet unidentified gunmen cut phone lines servicing the electric utility company PG&E Corporation's Metcalf transmission substation and disabled a transformer with machine gun fire. The incident has raised such high levels of concern, because it resulted in the disruption of electricity delivery to a number of strategic consumers in San Jose's Silicon Valley.

[19] An ancient military strategy of yielding ground to an adversary in order to gain time for mounting decisive counter-attacks, the defense in depth methodology has expanded to a variety of civilian applications including fire prevention, information assurance, and engineering. In the latter, an emphasis on redundancy allows a system to remain functional despite the failure of constituent components, instead of designing a single critical component that can never fail.

[20] While an advisable step toward improving the resilience of the grid, replacing coal and other fossil-fueled electricity generating facilities is now also of legal necessity in light of the Environmental Protection Agency's 2014 announcement that power plants across the U.S. must reduce carbon emissions by 30% by 2030.

lower cost. Similar to retiring the oldest equipment, putting lines underground is a sound improvement that eliminates one of the system's weakest points (i.e. exposed lines). While this presents a large up-front cost[70], it is a robust way to ensure the probability that downed power lines will not disrupt the grid's operation. However, these are essentially routine component upgrading and hardening measures that do little to advance the system-level resilience of the grid.

Some of the most promising progress in this regard is the increasingly granular level at which the state of the grid can be observed. The advent of phasor measurement unit (PMU) capability[71] enables system operators to record multiple observations of operational grid variables in a single second, whereas the conventional supervisory control and data acquisition (SCADA) system takes a single measurement every 2-5 seconds[72]. In light of the fact that the grid operates at many cycles per second, such an increase in granularity facilitates a more precise understanding of the dynamics at work within the system. When multiple PMUs are linked, operators can benefit from a more comprehensive view of what is happening across the grid through wide area measurement systems (WAMS)[73]. Such capabilities constitute the sensory component of the "sense and respond" paradigm that will be discussed further in the following section.

V. AREAS FOR FUTURE WORK

The ability to more quickly and accurately sense the occurrence of destabilizing events on the grid is a positive development, and one that will greatly enhance the grid's resilience as it is coupled with flexible response mechanisms distributed throughout the system to enable adaptive action[74]. Like an autonomic nervous system (ANS) for the grid, a computer-assisted dynamic fine-tuning or "sense and respond" capability will facilitate the timely identification of unstable conditions and enable automated corrective action. Just as the ANS functions below the level of consciousness to regulate basic bodily functions, a "sense and respond" capability will enable the grid to self-regulate by responding to disturbances faster than would be humanly possible. Still, extreme anomalies will undoubtedly require human intervention, and in such cases this advanced sensory and analytical capability will prioritize limited decision-making resources and drive better-informed action. Developing such an augmented intelligence[21] prioritization schema will be an important way to prevent decision or analysis paralysis[75][22], whereby decision makers become overwhelmed with such a deluge of information or *Big Data* that it becomes untenable to process all incoming sensory observations. In order to prevent decision paralysis, a robust sense and respond capability will help to determine which service disruption or other irregularity occurring on the grid is the most important problem, and thereby prioritize where grid operators would need to focus their remediation efforts. This sense and respond paradigm will be further explored in future papers.

Although equipping the grid with the ability to better sense the occurrence of destabilizing events and respond with corrective action is a large step forward, it does not neutralize the threat of IMDs. An expanded conception of the nature of threats to critical infrastructure is in order, which includes a wider consideration of the means available to bolster resilience. One option is to consider how carefully we monitor the distribution and sale of IMD components, akin to current efforts to track the movement of IED precursors. Such efforts bear similarity to the product recall functions of federal agencies like the Food and Drug Administration (FDA), the Department of Agriculture's Food Inspection and Safety Service (FSIS), the Center for Disease Control and Prevention (CDC), and the Department of Health and Human Services (HHS), who are responsible for implementing recalls of food, drugs, and other consumer products that pose a threat to citizens' health and safety. In the first quarter of 2014, the FDA managed 553 food, pharmaceutical, and medical device recalls, 38% of which involved products of international origin[76]. Despite such efforts, the CDC estimates that on a yearly basis, contaminated food kills 3,000 people and sickens another 48 million[77], and so clearly food recalls are not a perfect defense against contaminated food. While recall efforts have proved daunting in the past, the advent of collaborative big data analytics and high performance computing could offer new insights and avenues for tracking items of interest and intervening to mitigate against harm [78].

Similarly, big data analytics could be leveraged to identify potentially malicious actors. Much like the Coplink system used to such great effect amongst law enforcement agencies[79], the ability to assimilate data from various sources about individuals whose behavior and public statements suggest they pose a threat to critical infrastructure could be relayed to appropriate authorities for further investigation and/or action. For example, incident reports or other records of an individual caught attempting to access critical infrastructure facilities without clearance, making unofficial inquiries about critical infrastructure systems without a demonstrably legitimate purpose, or making public statements in social media or elsewhere regarding threats to critical infrastructure would feed into an alert system integrated with existing critical infrastructure information systems. Should an individual's behavior raise sufficient suspicion as determined by an established fact management framework, red flags would trigger action on the part of appropriate authorities. As Coplink has become the "google for cops", and proven effective at data integration and knowledge management for decision support[80], so too could such a mechanism support CIP.

[21] In contrast to Artificial Intelligence, Augmented Intelligence is an alternative AI, which is less romanticized by science fiction and more informed by practical experience. It refers to the logical union of machine capability with human intuition, suggesting that despite the advancement of technological capability, human critical thinking capability will maintain a role in nearly all aspects of critical infrastructure and other decision making processes.

[22] Coined by prominent psychologist Barry Schwartz, Decision Paralysis refers to the phenomenon in which an overabundance of choice exacerbates indecision and impedes decisive action.

VI. CONCLUSION

The complexity of modern critical infrastructure systems is both an asset and a liability. The increasing reliance on sophisticated technology enables more efficient operation, yet also leaves systems vulnerable to attack and cascading failure. Technology is central to nearly every aspect of our personal and professional lives, and so the electric grid that powers such technology must operate constantly without disruption. However, the grid does not operate in a vacuum, and an increasingly large set of variables affect its reliable operation. A grid system whose sole defense is the physical hardening of its key components against external threats is actually brittle, and only as strong as its most vulnerable component. CIP efforts will benefit from an expanded defense paradigm that also includes mechanisms to increase collective internal resilience of the system as a whole.

In order to build a more resilient electric grid, we must find new methodologies for discovering and analyzing the complex web of variables that have the potential to disrupt the grid's normal function, and architect a comparably robust set of protections to mitigate against them. The interdisciplinary nature of Sensemaking is ideally suited to meet such a challenge, in that this methodology incorporates a variety of mathematical, scientific, historical, sociological, and other perspectives, in order to gain deep insight into the nature of complex systems, thus illuminating viable decision pathways for strengthening the defense of systems. There is no single solution to the problem of CIP. Rather, a mixed-methods approach that derives wisdom from across professions and scholarly disciplines is particularly appropriate.

Just as modern civilization developed the skyscraper through the union of the architect's artistic vision and the builder's practical know-how, we can achieve more resilient critical infrastructure systems by uniting the art of human ingenuity and insight with the science that powers the grid and other related systems. Collaborative Big Data Analytics offers the capability to understand the persistent challenge of vulnerable critical infrastructure from a new vantage point. By offering the possibility of synthesizing, in real time, a virtually infinite range of information relevant to the operation of the grid, from weather and seismic data indicating the condition of the physical environment, to human-generated content, this methodology offers new insights to understanding trends in sentiment and intent to interfere with the grid. Sensemaking is a tool that offers great promise for leveraging large amounts of data to build more resilient and sustainable operating archetypes. We look forward to exploring these concepts more deeply in future work and demonstrating the value of Sensemaking as a methodology.

ACKNOWLEDGMENT

We would like to thank The Adjutant General of the State of Hawaii's Department of Defense and the Strategic Partnerships Office of U.S. Pacific Command (PACOM). Special thanks go to our inspiring force, and the Advisory Board Members of the Sensemaking/PACOM Fellowship, which is currently anchored at Swansea University's Network Science Research Center.

REFERENCES

[1] H. J. Rittel and M. Webber, "Dilemmas in a general theory of planning," *Policy Sciences,* vol. 4, pp. 155-169, 1973/06/01 1973.

[2] W. Weaver, "Science and Complexity," *American Scientist,* vol. 36, pp. 536-544, 1948.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks,* vol. 54, pp. 2787-2805, 2010.

[4] "U.S. Congress Office of Technology Assessment "Physical Vulnerability of Electric System to Natural Disasters and Sabotage" OTA-E-453," ed. Washington, DC: U.S. Government Printing Office, 1990.

[5] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," ed: USA - Canada Power System Outage Task Force, 2004.

[6] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur*, et al.*, "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *Power Systems, IEEE Transactions on,* vol. 20, pp. 1922-1928, 2005.

[7] J. Minkel. (2008) The 2003 Northeast Blackout--Five Years Later. *Scientific American*. Available: http://www.scientificamerican.com/article/2003-blackout-five-years-later/

[8] J. E. Dagle, "North American SynchroPhasor Initiative," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 2008, pp. 165-165.

[9] B. Everett. (2012, April 18, 2012) Ray LaHood: "America's One Big Pothole Right Now". *Politico*. Available: http://www.politico.com/news/stories/0412/75319.html

[10] G. Palla, I. Derenyi, I. Farkas, and T. Vicsek, "Uncovering the overlapping community structure of complex networks in nature and society," *Nature,* vol. 435, pp. 814-818, 2005.

[11] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability Engineering & System Safety,* vol. 121, pp. 43-60, 2014.

[12] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E,* vol. 69, p. 025103, 2004.

[13] *H.R. 5005-11 Critical Infrastructure Information Act of 2002,* U. S. Congress, 2002.

[14] M. Amin and J. Stringer, "The Electric Power Grid: Today and Tomorrow," *MRS Bulletin,* vol. 33, pp. 399-407, 2008.

[15] "U.S. Global Change Research Program National Climate Assessment," ed, 2014.

[16] "Investigation of 2006 Oahu Island-Wide Power Outage " Hawaiian Electric Company PUC Docket Number 2006-0431, 2006.

[17] S. H. Strogatz, "Exploring complex networks," *Nature,* vol. 410, pp. 268-276, 2001.

[18] R. G. Little, "Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures," *Journal of Urban Technology,* vol. 9, pp. 109-123, 2002/04/01 2002.

[19] R. Bilham, "Lessons from the Haiti earthquake," *Nature,* vol. 463, pp. 878-879, 2010.

[20] S. N. Jonkman, B. Maaskant, E. Boyd, and M. L. Levitan, "Loss of Life Caused by the Flooding of New Orleans After Hurricane Katrina: Analysis of the Relationship Between Flood Characteristics and Mortality," *Risk Analysis,* vol. 29, pp. 676-698, 2009.

[21] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos: An Interdisciplinary Journal of Nonlinear Science,* vol. 17, pp. -, 2007.

[22] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," *The European Physical Journal B - Condensed Matter and Complex Systems,* vol. 46, pp. 101-107, 2005/07/01 2005.

[23] M. Van Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver, and E. Cruz, "THE STATE AND THE THREAT OF CASCADING FAILURE ACROSS CRITICAL INFRASTRUCTURES: THE IMPLICATIONS

OF EMPIRICAL EVIDENCE FROM MEDIA INCIDENT REPORTS," *Public Administration,* vol. 89, pp. 381-400, 2011.
[24] K. Kurokowa, "National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission Report," ed, 2012.
[25] G. J. Fryer, P. Watts, and L. F. Pratson, "Source of the great tsunami of 1 April 1946: a landslide in the upper Aleutian forearc," *Marine Geology,* vol. 203, pp. 201-218, 2004.
[26] Y. Y. Haimes, K. Crowther, and B. M. Horowitz, "Homeland security preparedness: Balancing protection with resilience in emergent systems," *Systems Engineering,* vol. 11, pp. 287-308, 2008.
[27] F. L. Nathan, V. Paul, and J. P. Tony, "The state of the art in biomimetics," *Bioinspiration & Biomimetics,* vol. 8, p. 013001, 2013.
[28] Z. Anwar, M. Montanari, A. Gutierrez, and R. H. Campbell, "Budget constrained optimal security hardening of control networks for critical cyber-infrastructures," *International Journal of Critical Infrastructure Protection,* vol. 2, pp. 13-25, 2009.
[29] J. M. Boggess, G. W. Becker, and M. K. Mitchell, "Storm & flood hardening of electrical substations," in *T&D Conference and Exposition, 2014 IEEE PES*, 2014, pp. 1-5.
[30] I. M. Gibson, "The Maginot Line," *The Journal of Modern History,* vol. 17, pp. 130-146, 1945.
[31] W. Allcorn, *The Maginot Line 1928–45*: Oxford: Osprey Publishing, 2003.
[32] P. G. Bennett and M. R. Dando, "Complex Strategic Analysis: A Hypergame Study of the Fall of France," *The Journal of the Operational Research Society,* vol. 30, pp. 23-32, 1979.
[33] P. Sung Min, P. Sung-Yeul, Z. Peng, P. Luh, M. T. J. Rakotomavo, and C. Serna, "Comparative life cycle cost analysis of hardening options for critical loads," in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, 2014, pp. 1-5.
[34] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy,* vol. 39, pp. 6100-6119, 2011.
[35] J. C. Burnham, "New Perspectives on the Prohibition "Experiment" of the 1920's," *Journal of Social History,* vol. 2, pp. 51-68, 1968.
[36] W. Hall, "What are the policy lessons of National Alcohol Prohibition in the United States, 1920–1933?," *Addiction,* vol. 105, pp. 1164-1173, 2010.
[37] M. Thornton, *The Economics of Prohibition*: University of Utah Press, 1991.
[38] V. W. Peterson, "Chicago: Shades of Capone," *The ANNALS of the American Academy of Political and Social Science,* vol. 347, pp. 30-39, May 1, 1963 1963.
[39] *Dr. Bob and the Good Oldtimers*: Alcoholics Anonymous World Services, New York, NY, 1980.
[40] P. Gill, J. Horgan, and J. Lovelace, "Improvised Explosive Device: The Problem of Definition," *Studies in Conflict & Terrorism,* vol. 34, pp. 732-748, 2011/09/01 2011.
[41] C. Russell, "GAO 12-280 Warfighter Support: DoD Needs Strategic Outcome-Related Goals and Visibility over Its Counter-IED Efforts," U.S. Government Accountability Office, Washington D.C.February 2012 2012.
[42] G. Zorpette, "Countering IEDS," *Spectrum, IEEE,* vol. 45, pp. 26-35, 2008.
[43] S. T. Chung, Y. Yoon, and H. J. Park, "Screening and prioritizing the precursors of improvised explosive devices from commodity chemicals being controlled under Korean regulations," *Journal of Loss Prevention in the Process Industries,* vol. 26, pp. 1679-1684, 2013.
[44] P. Kolesar, K. Leister, D. Stimpson, and R. Woodaman, "A simple model of optimal clearance of improvised explosive devices," *Annals of Operations Research,* vol. 208, pp. 451-468, 2013/09/01 2013.
[45] (2013) White House Policy Statement on Countering Improvised Explosive Devices. Available: http://www.whitehouse.gov/sites/default/files/docs/cied_1.pdf
[46] D. Kotz, "Injury toll from Marathon bombs reduced to 264," *The Boston Globe,* vol. 24, 2013.
[47] "Counter-Improvised Explosive Device Strategic Plan," U. S. DoD, Ed., ed: Joint Explosive Device Defeat Organization, 2012.
[48] D. T. Kuehl, "Airpower vs. electricity: Electric power as a target for strategic air operations," *Journal of Strategic Studies,* vol. 18, pp. 237-266, 1995/03/01 1995.
[49] R. A. Pape, "The limits of precision‐guided air power," *Security Studies,* vol. 7, pp. 93-114, 1997/12/01 1997.
[50] T. W. Smith, "The New Law of War: Legitimizing Hi–Tech and Infrastructural Violence," *International Studies Quarterly,* vol. 46, pp. 355-374, 2002.
[51] I. Bonsen, "The Tesla Effect: Electronic Terrorism and Directed Energy Weapons," *CBRNePortal Editorial,* April 29, 2014 2014.
[52] J. A. Olsen, *John Warden and the Renaissance of American Air Power*: Potomac Books: Washington D.C., 2007.
[53] S. Graham, "Switching cities off," *City,* vol. 9, pp. 169-194, 2005/07/01 2005.
[54] J. F. Schneider and C. A. Brown, "Method of disrupting electrical power transmission," ed: Google Patents, 2011.
[55] C. A. Wargo, G. C. Church, J. Glaneueski, and M. Strout, "Unmanned Aircraft Systems (UAS) research and future analysis," in *Aerospace Conference, 2014 IEEE*, 2014, pp. 1-16.
[56] R. Clarke and L. Bennett Moses, "The regulation of civilian drones' impacts on public safety," *Computer Law & Security Review,* vol. 30, pp. 263-285, 2014.
[57] E. Bompard, T. Huang, Y. Wu, and M. Cremenescu, "Classification and trend analysis of threats origins to the security of power systems," *International Journal of Electrical Power & Energy Systems,* vol. 50, pp. 50-64, 2013.
[58] R. Smith. (2013, February 13, 2013) Assault on California Power Station Raises Alarm on Potential for Terrorism. *Wall Street Journal*. Available: http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778
[59] J. Peppard, ""Reward Offered in Power Transformer Shooting,"" in *WTSP News (Tampa)*, ed. Tampa, 2005.
[60] M. Brantley, ""FBI Reports Three Attacks on Power Grid in Lonoke County,"" in *Arkansas Times*, ed, 2013.
[61] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences,* vol. 108, pp. 3838-3841, March 8, 2011 2011.
[62] P. Parfomak, "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations," Congressional Research Service, Washington D.C.2014.
[63] "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments," N. S. Agency, Ed., ed, 2001.
[64] A. Ipakchi and F. Albuyeh, "Grid of the future," *Power and Energy Magazine, IEEE,* vol. 7, pp. 52-62, 2009.
[65] V. Vittal, "The impact of renewable resources on the performance and reliability of the electricity grid," *The Bridge,* vol. 40, pp. 5-12, 2010.
[66] H. Haibing, S. Harb, N. Kutkut, I. Batarseh, and Z. J. Shen, "A Review of Power Decoupling Techniques for Microinverters With Three Different Decoupling Capacitor Locations in PV Systems," *Power Electronics, IEEE Transactions on,* vol. 28, pp. 2711-2726, 2013.
[67] Z. Popovic and V. Cackovic, "Advanced Metering Infrastructure in the context of Smart Grids," in *Energy Conference (ENERGYCON), 2014 IEEE International*, 2014, pp. 1509-1514.
[68] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology,* vol. 19, pp. 105-120, 2014.
[69] R. E. A. Harder, K. Peterson (2014, 1 June 2014) EPA to Seek 30% Cut in Emissions at Power Plants. *Wall Street Journal*. Available: http://online.wsj.com/articles/epa-carbon-emissions-rules-carry-political-risks-for-some-democrats-1401658355
[70] B. J. McNair, J. Bennett, D. A. Hensher, and J. M. Rose, "Households' willingness to pay for overhead-to-underground conversion of electricity distribution networks," *Energy Policy,* vol. 39, pp. 2560-2567, 2011.
[71] A. G. Phadke, "Synchronized phasor measurements-a historical overview," in *Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES*, 2002, pp. 476-479 vol.1.
[72] M. Padmanaban and A. K. Sinha, "Adaptive power system hybrid state estimation," in *Innovative Smart Grid Technologies - Asia (ISGT Asia), 2014 IEEE*, 2014, pp. 680-685.
[73] A. G. Phadke and R. M. de Moraes, "The Wide World of Wide-area Measurement," *Power and Energy Magazine, IEEE,* vol. 6, pp. 52-65, 2008.

[74] M. Amin, "A Smart Self-Healing Grid: In Pursuit of a More Reliable and Resilient System [In My View]," *Power and Energy Magazine, IEEE,* vol. 12, pp. 112-110, 2014.
[75] B. Schwartz, *The Paradox of Choice: Why More is Less* Harper Perennial, 2004.
[76] "Quarter 1 Recall Index," Stericycle Expert Solutions2014.
[77] D. B. J. Cascone, K. Ferrara, E. Gauthier, C. Henry, "Food Safety: A Year in Review," Deloitte Development LLC2013.
[78] C. O. T. Wynn, A. Hofstede, C. Fidge "Data and process requirements for product recall coordination," *Computers in Industry,* vol. 7, pp. 776-786, 2011.
[79] R. V. Hauck, H. Atabakhsb, P. Ongvasith, H. Gupta, and C. Hsinchun, "Using Coplink to analyze criminal-justice data," *Computer,* vol. 35, pp. 30-37, 2002.
[80] P. J.-H. Hu, H. Chen, H.-f. Hu, C. Larson, and C. Butierez, "Law enforcement officers' acceptance of advanced e-government technology: A survey study of COPLINK Mobile," *Electronic Commerce Research and Applications,* vol. 10, pp. 6-16, 2011.