AU/ACSC/2018

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CROSS-DOMAIN DETERRENCE TO PROTECT THE U.S. ELECTRICAL GRID

by

James H. Nicholas, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Dr. Andrew Niesiobedzki & Dr. William Hanson

Maxwell Air Force Base, Alabama

June 2018

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

ABSTRACT

The United States, now more than ever, is extremely reliant upon dependable delivery of electricity from the national electric grid. In order to preserve this critical national infrastructure, the U.S. needs to strengthen its cross-domain deterrence posture to protect the grid as components and control mechanisms become increasingly vulnerable and attractive for adversaries to exploit.

A problem/solution framework will assess proposed measures the U.S. can implement to deter adversaries from future attacks on the U.S. electrical grid. Also addressed are the grid's background and development, vulnerabilities within the infrastructure, as well as the effectiveness of current deterrence measures. Research shows that modern physical protection measures are naively simplistic, that "cyber smart practices" for network security lack industry standardization and compliance, and that deterrence strategies for the cyber domain lack credibility and action. Recommendations to increase future U.S. deterrence posture include: physical, hardware, software and training upgrades; an international coalition construct for cyber policing, enforcement and legitimacy; and, a Decision Authority-ID-ROE matrix that provides a framework and delegated authority for cyber defenders to engage in persistent deterrence and enforcement operations.

Introduction

The United States has evolved over the last century into one of the most technologically advanced and interconnected societies on the planet. As a result, reliable delivery of electricity forms a foundation for America's economy, national security, as well as the health and safety of its citizens. The U.S. electric grid not only provides the power which runs modern society, but also has itself become increasingly reliant upon the energy it provides and the technology it enables in order to operate. An aging infrastructure, as well as unprotected nodes and elements within the grid's architecture, compounded by an increasing reliance on modern computer control systems, has created new and exploitable vulnerabilities. This publicly-acknowledged weakness creates an inviting target set for both state and non-state actors who wish to harm the United States.

Current deterrence models do not adequately protect many of the grid's vulnerabilities because they evolved from a Cold War nuclear mindset, which seeks to avoid conflict altogether by promising retaliation. In contrast, cyber and physical attacks are already taking place, but they typically occur below a threshold that warrants military response. Therefore, this paper seeks to address shortcomings in current deterrence theory and recommend measures the U.S. can put in place for future electrical grid security.

Potential physical attack mechanisms to exploit electrical grid infrastructure vulnerabilities can range from explosives and firearms to nuclear detonations with a damaging electromagnetic pulse, and are fairly straightforward. As such, society is likely to back a governmental retaliatory response, and numerous recommendations exist which address these threats. Another primary vulnerability, however, resides in the computer control systems which govern and regulate the U.S. network: Supervisory Control and Data Acquisition / Energy

Management Systems (SCADA/EMS). Incorporated into the electrical grid to run operations with greater efficiency than previous mechanical or analog systems, these systems were not designed to be protected against the current and future cyber threats of the growing internet era.

Further exacerbating this issue is a lack of clear guidance and understanding about how to regulate and respond to threats in the cyber domain. Unlike a physical attack, cyberattacks against the electrical grid occur on a daily basis and, due to the complex and anonymous nature inherent in the cyber realm, these attacks often go unpunished.[1] These factors combine to create a significant deterrence problem for the U.S.

When considering how to develop a deterrence posture against cyber threats, the factors of attribution and retribution must be explored. Identifying the origin of an attack or threat is a primary concern, but consideration must also be given to protecting the nature of U.S. capabilities when conclusively identifying and locating such perpetrators. If sufficient capabilities to properly track and identify threat actors do not presently exist, a future (and ongoing) recommendation will be for advancements in cyber-security development. Other solutions could include the development of an identification or response matrix, providing a graduated response option list as well as listing key trigger events that identify U.S. thresholds for action. With the help of America's military strengths, cross-domain response options will be factored in when and where necessary to optimize a deterrence posture.

While areas for future consideration should continue to examine developing threats as technology and internet exploitive capabilities evolve, the viability of a "cyber response coalition" construct should also be considered. Creating a multi-nation team, with information-sharing agreements cultivates a collaborative effort to respond to cyberattacks against coalition partners. Such a construct could have compounding benefits beyond cyber-security, such as financial savings from asset and capability-sharing, strategic basing opportunities, and increased international legitimacy when confronting threat actors.

A problem/solution framework will be used to guide this research paper. Following a short background describing the U.S. electrical grid infrastructure, the paper will discuss vulnerabilities, both current and expected, as well as U.S. deterrence postures and response options against potential adversary actions. The effectiveness of current deterrence and physical protection measures against future adversaries will be assessed throughout this discussion. Shortfalls will be compared against alternative deterrence or protection possibilities and recommendations will be made for future improvement.

In response to the question "What measures can the U.S. put in place to deter future adversaries from attacks on the U.S. electrical grid?" this paper will illustrate how current deterrence measures and physical protections are minimally effective against ongoing and future threat attacks. Recommendations for both a cyberattack decision matrix as well as a coalition cyber policing task force will enable faster retribution response times - thereby discouraging subsequent attacks - and provide the legitimacy of a unified international community response.

Literature Review

The U.S. national electrical grid is a critical infrastructure that supports the day-to-day operations, health, welfare and economic power of the country. Accordingly, there is no shortage of literature discussing the current state and future of this machine. The sources used in this paper can be broken down into five sections: overall electrical grid infrastructure, its age and importance to protect; physical challenges and safeguards for the grid; cyber concerns or threats; cyber deterrence and the concept of a new domain in future warfare; and miscellaneous sources that provide some background for the proposed solutions.

Electrical Grid Infrastructure and Importance

President Trump's *The National Security Strategy* (NSS) and Defense Secretary Mattis' *The National Defense Strategy* (NDS) provide a foundation for the overall problem as well as the importance of addressing it by laying out potential problems that the U.S. must address in the near future in order to protect itself. Both describe the national electrical grid as critical and at risk of malicious attack, especially with the increased reliance on digital technology. The NDS highlights which actors pose the greatest threats, while the NSS acknowledges that deterrence responses will come from all domains of national power projection.[2] Neither document issues specific guidance for addressing these threats and vulnerabilities; they are simply used to make the American public aware. Further, an acknowledgement that "deterrence today is significantly more complex to achieve" helps underscore this paper's recommendation for a pre-determined response matrix which national leadership can confidently rely upon in a future of ambiguity.[3]

Other sources that provide a good overview on how the electrical grid's infrastructure developed include the U.S. Energy Information Administration's (EIA) website, Will Daugherty's summary of the *Lloyd's Report* and Gellings and Yeager's *Transforming the Electric Infrastructure*. The EIA website is an authoritative source of information about how the modern electrical grid system works in the U.S., how electricity is delivered to consumers and how electrical systems are interconnected into larger, more reliable networks.[4] Combining this with Daugherty's report helps to explain overarching concepts and recommendations for strengthening the electrical grid against future vulnerabilities.[5] Gellings/Yeager's article gives essential background on how the electrical grid was developed, evolved over time and works today. In addition, they address numerous factors about the current state of the grid as well as sustainment and improvement considerations for future infrastructure survival.[6] Knowing how the electrical grid came to be is essential for understanding how to protect it in the future.

Physical Challenges and Safeguards

A comprehensive evaluation done by McLarty and Ridge, *Securing the U.S. Electrical Grid*, as well as news sources from Behr and Harris illustrate that the physical longevity of the grid is dependent on increasing protection measures and replacement of aging components. McLarty and Ridge, as part of the Center for the Study of the Presidency & Congress, present a thorough study on threats to the grid's effectiveness as a critical national infrastructure component and how to ensure its future security through modernization.[7] They touch not only on the grid's physical deficiencies but also the increasing vulnerabilities of its cyber components. Behr and Harris present news articles that capture the details of two very simple, but effective rifle attacks on substations in California and Utah that stand as a warning for how vulnerable some of the grid's components may be to physical attack, to include the potential widespread implications for those reliant on power sources.[8]

Cyber Concerns or Threats

While the need to protect our grid infrastructure against physical attacks that cause considerable damage is easily understood, it is more difficult – and thus a new and vibrant topic of discussion and research – to realize how the electromagnetic and digital realms of the cyber-enabled world we live in could be impacted, including the 2nd and 3rd order of effects, from a corresponding "invisible" attack. With this in mind, there is a considerable amount of literature on the topic of cyber warfare or cyberattack and its implication on national strategy and infrastructure, as well as how to address the issue of deterrence with respect to this emerging domain. Common recommendations to increase U.S. deterrence for grid security include physical upgrades and standardization efforts that have been known for years; however, because the newer cyber realm has such a significant enabling function for command and control (C2), a majority of research and discussion will be focused on this vulnerability.

The Idaho National Laboratory's *Cyber Threat and Vulnerability Analysis* provides a primary source of reference on the vulnerabilities and threats in the cyber domain to the U.S. electric grid. As part of the U.S. Department of Energy's national laboratories complex, the Idaho National Laboratory (INL) has specific interest in the energy and national security interests of the U.S. In addition, the authors have an insider's knowledge of the electrical grid infrastructure, capabilities and redundancies as well as current threats, vulnerabilities and limitations. The report provides a comprehensive background on how the electrical grid works and the vulnerabilities introduced as part of the expanse of automation and electronic control mechanisms.[9] *Cyber Threat* also details the current and ongoing attacks that plague the electrical grid as well as limitations on how localized electric sectors control modernization protection efforts.[10] Finally, this report strengthens the argument that national decision makers should be armed with definitions and pre-determined response options to attacks on the grid.

Robert Knake's *Cyberattack on the U.S. Power Grid* memorandum provides useful research and recommendations from the Council on Foreign Relations (CFR), with both an argument for the importance of protecting critical U.S. infrastructure, as well as a moderate assessment of which countries are likely to pose a threat.[11] Further, he alleges "adversaries may underestimate" capabilities the U.S. have in place to counter and deter hostile attacks.[12] The CFR memo also supports the proposal that the U.S. government should have pre-determined response measures in place. Finally, this memo advocates for improving physical security measures that can be immediately implemented, to reinforce a U.S. cyber deterrence posture.[13]

The NSS Labs Report *Vulnerability Threat Trends* by Stefan Frei is an original study evaluating disclosed cyber vulnerabilities contained in the national vulnerability database. NSS Labs drew comparisons across the various industries to find trends and assess vulnerabilities based on assigned critical levels and attack complexities to determine where significant problems lie.[14] Also assessed were computer applications and web browsers that experience the most vulnerability issues, which were then compared to the SCADA systems of issue for the electrical grid analysis.[15] Fink, Spencer and Wells' *Lessons Learned from Cyber Security Assessments of SCADA and EMS* report is a condensed summary of ten independent assessments performed within DOE and DHS from 2004-2006. A primary focus of the assessments was on SCADA/EMS systems because of their networking nature. After analysis of the various studies, a list was compiled of vulnerabilities and recommended solutions for the future security of electrical grid components.[16]

A RAND Strategic Appraisal study written by Zalmay Khalilzad, *Defense in a Wired World: Protection, Deterrence, and Prevention,* discusses the changing dynamics of information in warfare and talks about the issues of protection, deterrence and defense of US interests from attack through the information or cyber realm.[17] While a bit dated in its information about capabilities, the overall concepts of how to attribute a threat actor and how to protect against or deter that actor from attacking critical information infrastructure components still warrant consideration. Khalilzad makes a very clear argument about how deterrence from information warfare is considerably more difficult to conceptualize and implement than previous deterrence ventures against tangible warfare like nuclear exchange.[18] In a similar venture, James Clapper's statement *Worldwide Cyber Threats* – as a former Director of National Intelligence – is an official assessment of the threats faced by the cyber realm. It includes a discussion of the risks and costs as well as evolving capabilities to track and attribute crimes to threat actors, giving a summary of the primary threat actors that are of immediate concern.[19]

A final reference on cyber protections is the Lloyd’s Emerging Risk Report *Business Blackout*, which was generated to illustrate the impact a cyberattack could have on the population/economy, where insurance companies may incur liability to cover people’s losses. From that perspective, a worst-case scenario was presented in order to highlight compounding orders of effects, with appropriate caveats. The overall picture painted shows a significant economic impact on the affected areas of the country. On the positive side, research highlighted that there is inherent security and resiliency within the electrical grid based on the variability of the power sources and layered construction of many network components.[20]

Cyber Deterrence and the Cyber Domain

Related to articles about cyber protections is a smaller subset of material discussing the specific role of deterrence in the cyber realm. Vincent Manzo’s *Deterrence and Escalation in Cross-Domain Operations* highlights some of the difficulties in proposing and carrying out deterrence measures across the lines of different domains. Manzo illustrates that much of the warfare operations the U.S. faces today are inherently cross-domain, and that the American way of approaching deterrence and retaliation responses is done with minimal consideration for crossing the domain boundaries.[21] He further illustrates, however, that typical human nature has a tendency to keep responses within the same type of domain in which an attack came from.[22] The concern is that U.S. responses to an adversary’s attack may not trigger the deterrence response that was hoped for; an adversary from a different world or culture may not correctly associate U.S. action as being in response to their action. Manzo clarifies that, for deterrence measures to be taken at the intended face value (and indeed to be most effective), there needs to be a shared framework, so that all parties involved understand what actions are related.[23] This notion supports a recommendation of publicized response options (via the decision matrix) as a better means to broadcast U.S. deterrence in the protection of its interests.

Cilluffo and Cardash's *Cyber Domain Conflict in the 21st Century* discusses how the cyber domain has become a new medium for conflict, how adversaries seek to use cyber benefits to their advantage, particular abilities that are enabled/strengthened through cyber, as well as what vulnerabilities that poses for the U.S. Questions posed by the authors at the article's conclusion provide justification for some of the deterrence measures proposed in this paper, such as "Should there be a greater role for active defense, meaning the ability to immediately attribute and counter attacks, in order to address future threats in real-time?" as well as "What should U.S. rules of engagement look like?"[24] They also highlight that deterrence and defense in the cyber realm requires a multinational effort.

Kenneth Geers' article "The Challenge of Cyber Attack Deterrence" considers variables involved when developing deterrence strategies for a nation-state, specifically that denial and punishment strategies are the only viable options applicable to the cyber domain.[25] He highlights many of the problems associated with traditional deterrence constructs as applied to the cyber domain and lists key issues that must be addressed in future cyber doctrine. Other than listing key issues, there are no proposed solutions; however, his arguments substantiate this paper's proposal for an international cyber effort as well as the civilian-military communications necessary to effectuate the decision matrix.

Jacquelyn Schneider's draft chapter for *Cross-Domain Deterrence: Strategy in an Era of Complexity* seeks to define how cyberspace qualifies as a domain versus an infrastructure and the subsequent implications when addressing deterrence, specifically the complications that arise because it serves as both.[26] This conflicting U.S. view is then contrasted to that of near-peers Russia and China; since they do not interpret cyberspace the same, we cannot assume a deterrence model that fits a western-only view.[27] Schneider's discussion of how and why it is important to correctly frame cyberspace is especially useful when considering cyber deterrence theory, in order to ensure deterrence measures are correctly paired to desired end-state goals.[28]

The final reference on cyber deterrence, Fischerkeller and Harknett's "Deterrence is not a Credible Strategy for Cyberspace," discusses various strategies as applied to cyberspace. They argue that, due to the uniqueness of cyber, different considerations and approaches should apply.[29] Specifically, they state that the current strategy of operational restraint is counterproductive and actually hinders deterrence in cyber.[30] Many repeated issues plaguing deterrence theories are highlighted and then applied against the proposed idea of cyber persistence. This cyber persistence requires modifying authority delegation, enabling more presence and posturing in the cyber domain and acceptance of a new method of deterrence for a future digital world.[31] Persistent cyber presence, cooperation, and communication fit into the decision/authority matrix proposed in this paper as they are key factors to its operational success.

Miscellaneous Sources Supporting Recommendations

Finally, resources that provide background information to support proposed deterrence recommendations include CJCSI 3121.01A *Standing Rules of Engagement for US Forces*, which "establishes SecDef-approved standing rules of engagement (ROE) that…provides guidance for the application of force for mission accomplishment," and AFTTP 3-1.General Planning Attachment 2, which provides guidance for identification criteria in an air-to-air or air-to-ground environment.[32] Together with theater-specific ROE, combatants use this guidance as a decision matrix to determine if offensive/retribution actions can be taken against hostile threat actors.

Using a construct already accepted and understood by Air Force personnel, a derivative matrix will be constructed as an example for how to establish future cyber defensive and offensive actions which could increase deterrence against hostile threat actors who wish to exploit the cyber domain as means to cause damage to U.S. national interests.

Background of the U.S. Electrical Grid

Before an effective discussion can be had about deterrence against attacks on the electrical grid, it is helpful to understand how it was developed and has grown into the complex that we know today. Since 1881 when Thomas Edison designed and established the first power company, the U.S. electrical grid has grown tremendously. Although there are still remnants of that original network providing power to some 2,000 homes, the vast expansion began in the 1930s and saw significant development throughout the 1950s and 1960s.[33] As the demand for electricity grew and technology advanced to be able to send it further and reach into every home, the physical growth of the network was largely a process of adding on to, or building on top of, old networks as each new capability emerged and then growing outward to reach every community. In this fashion, the electrical grid was not designed from any one point in time, where modern technology was available to build a universally seamless and integrated network. Consequently, many of the power delivery systems are based on 1950's or earlier technology, much of the equipment has been operating for 50+ years, and safeguards or protection measures against possible attacks were not inherently designed into the system.[34]

Today's electricity system, often described as "the most complex machine ever built," includes over 200,000 miles of high-voltage transmission lines, millions of miles of low-voltage distribution wires, transformers and substations, and serves over 300 million consumers.[35] Energizing the grid are thousands of power plants, ranging from fuel-driven sources like nuclear, oil, coal and natural gas, to environmental sources like hydropower, solar, geothermal and wind. Balancing supply and demand, along with parameter tolerances, becomes increasingly critical in order to prevent failures, faults or surges from shutting down local networks which could, in turn, propagate to area blackouts.[36] To help prevent disturbances, industrial size circuit breakers and relays help manage current and loading, and power plants/distribution centers are being upgraded to higher levels of sophistication and automation via SCADA/EMS computers. The latest trend in efficiency and management is the so-called "smart grid" technology, "which allows utilities and customers to receive information from and communicate with the grid."[37] All of these advancements help to optimize the delivery and demand of U.S. electricity requirements, which totaled 3.82 trillion kilowatt-hours (kWh) and cost over $400 billion in 2017.[38] However, the vast layout of its design and the increasing reliance upon technology has created vulnerabilities in the 21st century that Edison and his team could never have imagined.

Management of the electrical enterprise has developed into an aggregate in a similar fashion as the physical network's growth. One hundred years ago, there were "more than 4,000 individual electric utilities operating in isolation from each other," but as demand grew the companies interconnected their physical transmission networks in order to increase service reliability and efficiency at a reduced cost.[39] Today, there are three primary, large interconnected systems covering the U.S. – subdivided into eight regional reliability councils and approximately 150 control area operators, which distribute electrical supply to consumers. Further complicating the business, there are over 3,000 companies owned or managed by investors, municipalities, cooperatives and federal agencies.[40] With regional connectivity, consumers today benefit from lower costs and greater reliability than any previous generation. These variations in ownership entities, combined with a lack of government mandates, have resulted in vulnerabilities due to a lack of standardization and interoperability between sectors. Though numerous standards and recommendations have been published to make companies aware of these infrastructure and technology updates, vulnerabilities, and physical and cyber threats, the actual compliance and implementation of these standards is voluntary. In the name of profit, many companies have chosen to forgo costly improvements, leaving consumers unaware of how fragile their electrical supply may be.

Problem and Key Issues

Infrastructure Vulnerabilities

Today's electrical grid has two primary vulnerabilities: first, the physical infrastructure which is comprised of unprotected and aging components and covers a vast expanse across the country; second, is the interdependent connections that make up the network sectors, which are increasingly combined and then controlled by advanced SCADA/EMS systems. This evolution of technology is being further pushed towards more autonomy with "smart grid" component incorporation.

Physical infrastructure vulnerabilities were highlighted in 2013 and 2016, during which threat actors crippled two separate substations with simple high-powered rifles, neither of which has been properly attributed to the actors. These incidents serve as reminders that physical attacks can create significant potential damage, they can be coordinated with readily available munitions and do not require significant training or sophistication, and they can likely be executed in anonymity for the actors. The first of these attacks took place in 2013 near San Jose, California. During this event, the actors cut critical communications lines and then fired over 100 rounds from a high-powered rifle at several of the facility's transformers; the resulting leak of cooling oil caused the transformers to overheat and shut down, creating damages near $15 million.[41] A second attack came in 2016 in southern Utah, where another actor used a high-powered rifle to shoot holes in the oil-cooled radiator, again causing the transformer to overheat and shut down. The result of this attack was an electricity outage for 13,000 customers for one day and a six-month process to repair the transformer at a cost of $1 million.[42] Although neither of these attacks resulted in long-term power outages, they highlight the physical vulnerabilities that exist to hundreds more substations that make up the national electric grid. Many fear that these attacks were simply rehearsals or proof-of-concept drills to evaluate the effectiveness of such an attack. Should an adversary prove motivated enough, a well-coordinated attack on enough critical substations throughout the U.S. could result in a significant disruption of electricity for an extended period of time, with substantial cost for repair.

These transformer/substation hubs are ideal targets because they serve as critical nodes in the delivery system, few of them have "cameras, intrusion detection, or robust perimeter security," and there is a lack of hardening or walls to protect exposed vulnerable components.[43] Due to the nature of electricity delivery – wherein the entire purpose of the national grid is to transfer power generated over long distances to communities throughout – it would be cost-prohibitive and nearly impossible to provide physical protection to the entire network. In addition to deliberate acts to destroy critical equipment, many of the older components are also reaching their useful lives and are in need of upgrades or replacement. As stated earlier, the decision to modernize and repair worn out components falls on individual companies and – in the dynamic nature of business – the result is a spectrum of security and vulnerability between the different networks.

Although improbable, another physical vulnerability that cannot be forgotten is the significant damage an electromagnetic pulse (EMP) or directed energy (DEW) weapon would have on electrical grid components. While there would be other significant issues to contend with based on how such an effect was produced, such as through a nuclear detonation, recent rhetoric from hostile state actors to use such a weapon against the U.S. should not be outright dismissed and steps to mitigate its effect should be considered as part of a comprehensive and strategic approach to deterrence.

The second primary vulnerability to the U.S. electrical grid is technology, automation and connection to the internet or cyber domain. Continuing demand for electricity since the early 1900s has led to an evolution in ways to control and deliver it with maximum efficiency and reliability. The latest advancements in C2 are the SCADA/EMS systems, which provide a highly automated and reliable network of power. However, the very nature of SCADA/EMS is to be "interconnected with various data networks and with the networks that monitor and control critical infrastructure equipment…(which, if compromised) provide a path to many critical end devices."[44] These systems, while providing a significant advantage in efficiency and automation, were never designed to be connected to the internet and thus expose "vulnerabilities because they create the potential for attacks, launched from afar, to threaten…U.S. national security."[45] In addition, the next generation of "Smart Grid improvements will enable better monitoring, performance, and reliability of the system using thousands of remote-controlled measurement devices" controlled by a utility company from a central location.[46] As more devices and controls are plugged into the internet, more challenges in security arise "as these devices represent a new attack vector for malware or other disruptions."[47]

The significance of security risks from increased automation and network connectivity for the U.S. electrical grid is being realized as potential threat actors are "developing access to US infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile."[48] This is evident by the fact that many viruses known to have caused serious damage around the world were specifically designed to compromise SCADA systems.[49] A report from NSS Labs highlights that SCADA systems have been heavily scrutinized since the Stuxnet and Flame virus discoveries in 2010 and vulnerability disclosures have increased 600 percent from 2010 to 2012.[50] More alarming is that 90 percent of the disclosures are considered moderately or highly critical in nature, and another 9 percent of those disclosed in 2012 "are extremely critical paired with low attack/exploitation complexity.[51] Further supporting this trend, the Department of Homeland Defense has admitted that "cyberattacks on key energy infrastructure – particularly the electric system – are increasing in both sophistication," they are occurring on a daily basis, and they forecast that utility companies "are expected to spend about $7 billion on cyber-security by 2020."[52]

While the means to attack U.S. infrastructure are increasing in numbers and complexity, it is important to recognize why civilian networks may need to rely on military assistance in the future. Some nation-states have no reservations about blurring the lines between military and civilian employees engaging in cyber operations. As a result, it should come as no surprise that U.S. civilian infrastructure is not up to the task of defending against an adversary that is armed with military-grade equipment. Defense against this level of future threat will require significant civil-military cooperation.

Appeal of Attacking Electrical Grid Infrastructure

There are numerous reasons adversaries chose to attack America's electrical grid. Some envy the security, benefits and reliability that the U.S. electrical network provides, and some are paranoid from the modern era of real-time global reach and visibility that cyber and space capabilities allow. Regardless, America's capability to produce, dominance of, reliance upon, and hunger for electricity make it a premier target. However, the capabilities that this robust network enabled has, in turn, created a reliance and dependency throughout the fabric of American society that makes targeting it more appealing, and disrupting it that much more damaging. Further exacerbating the threat, younger generations increasingly take the modern electrified society for granted, unaware of how fragile systems may be in the wake of its loss, thus neglect to consider the importance of upgrading security measures and are wholly unprepared for a long-term power outage. The devastation resulting from a potent attack and long-term power outage would have dramatic consequences for the country and its stability.

Attacks on the physical infrastructure are appealing because of their simplicity to execute. The ease of obtaining firearms in America and lax security measures allow for a relatively low risk of punishment. Attacks on the grid from the cyber realm are becoming increasingly appealing to threat actors for a number of good reasons. First and foremost, the rise in automation via SCADA/EMS systems as well as the implementation of advanced "smart grid" technology opens up the possibility of attacking a majority of U.S. networks from anywhere around the world. Additionally, "once a sophisticated attacker uses a particular attack tool or exposes a particular vulnerability, it is out in the wild for others to grab and use, reverse engineer, or employ to (their) advantage."[53] Continuous advancement of technology and malicious code further helps threat actors remain anonymous and increases the ease and speed at which they can probe or attack U.S. systems.[54] Terrorists may find cyberattack mechanisms increasingly attractive because exploitation of "the power system's increasingly centralized control (can) magnify the effects of a localized strike."[55] Finally, attacks through the cyber realm "exponentially magnifies one of the hallmarks of terrorism…(that a) few can cause a degree of harm that is well out of proportion to the size of the attacking group."[56]

Current State of Deterrence

Defensive Protections

From a physical standpoint, the U.S. electrical grid has minimal protections on most grid components, primarily because the scale and reach of the physical infrastructure is far too vast to adequately put defenses around everything. However, even critical nodes such as substations or transformers often find themselves extremely vulnerable. With little more than barbed wire fences and surveillance cameras, these grid components are an inviting target set to an adversary who wishes to create havoc on U.S. soil as part of a comprehensive plan of attack. It is worth noting that the two recent attacks of 2013 and 2016, carried out with simple high-powered rifles, are a warning of the damage that a determined adversary with enough manpower could carry out. Additionally, if considering a future worst-case scenario of advanced weapons like High-Altitude EMP or DEW, most electrical grid components are not hardened adequately and could face catastrophic failures. Physically, the U.S. electrical grid has some inherent protections based on its sheer size and multiple redundancies. However, much of it is dated and could easily be damaged by a determined attack.

From a cyber standpoint, the U.S. electrical grid has similar inherent protections based on the variability of equipment, C2 systems, and networking setup. In other words, if an adversary were to develop a cyber weapon targeting one type of SCADA or grid component, generally that "weapon" would only work on that specific equipment, leaving redundant components built with a different C2 architecture unaffected. For a comprehensive attack, an adversary would need to gain access and develop programs designed against multiple systems and execute them in parallel to have a widespread effect. Additionally, "governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions."[57] From a vulnerability standpoint, the increasing push for automation and networking via "Smart

Grid" technology and implementation creates an easy avenue of attack, where "applications ranging from industrial sensors to home appliances, microprocessors now number more than 12 billion in the US alone."[58] In other words, the more that electrical grid C2 is networked through the internet, the greater future risks there are to cyber intrusion and attack.

In summary, the overall "vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication."[59] Even if the attacks are strictly targeting military sites, they will "likely traverse civilian networks" during the attack.[60] For these reasons, the U.S. should cooperatively prepare both civilian and military cyber defenders for a future of continued attacks on the grid.

Deterrence Effectiveness

Deterrence against small-scale physical attacks on U.S. electrical grid components is currently no greater than the deterrence our laws have against vandalism and destruction of property. Should someone get caught damaging a component of the grid, their arrest and punishment would be commensurate with the level of damage inflicted – criminal or felony – and state-sponsored attacks or terrorism can be downplayed or amplified depending on an adversary's wish. Recent attacks have shown that components are generally very easy targets and there is little repercussion because of the difficulty in securing the vast infrastructure as well as correctly attributing the actors responsible. Inherent in the size and redundancy of electrical production and distribution, some deterrence exists due to the number of critical nodes and delivery mechanisms. From a purely physical attack, an adversary would have to attack thousands of targets to effectively cripple the U.S. electricity infrastructure.

Deterrence against attacks in the cyber realm is very different, yet equally problematic. By continuing the trend towards increased automation and component integration, the electrical grid opens itself up to an exponential array of adversary avenues of attack. Most importantly, the adversaries don't need access to American soil to initiate their attacks and wreak havoc; they only need an internet connection, sophisticated equipment and competent training to gain access to many of our critical infrastructure components. Further, the cyber domain has proven to be fairly anonymous for an adversary to hide their activities within and provides an easy mechanism for indirect state sponsorship, while maintaining plausible deniability. In addition, "hackers are often able to gain access to their targets without having to resort to using advanced capabilities," highlighting that U.S. defenses and personnel training are lagging far behind the threat.[61] Also, "policymakers are uncertain about how to credibly threaten to impose costs on aggressors and deny benefits of attacks" against those that use cyberattacks on critical U.S. infrastructure.[62] With all of these problems being faced as the U.S. tries to comprehend and apply traditional theories of deterrence to the cyber domain, it is not surprising that anything "networked" will be at risk until an effective solution can be found.

Applying traditional deterrence to cyberspace, where one "seeks the absence of unwanted activity in an environment of constant activity," has proven to be a "comprehensive mismatch" and thus warrants a redefinition of deterrence as applied to cyber.[63] In other words, Cold War ideas imply that, if we generate enough might we can prevent attacks from taking place, but they do not adequately address deterrence in the cyber domain. The current U.S. posture of operational restraint is largely to blame for the effectiveness of our past deterrence posture in the battle to control cyber domains. Because this environment continues to be a place where actors will continue to test U.S. "technical capabilities, political resolve, and thresholds," a lack of response to daily attacks "has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation."[64] In summary, this trend of attacks without retaliation is creating a new environment in which the U.S. stands to lose a great deal of deterrence credibility if it cannot reverse the course on combating threats to its critical infrastructure components. Traditional deterrence, as applied to the cyber realm, has not proven to be an effective strategy.

Alternatives

Defensive Protection Measures

The previously reviewed literature makes numerous recommendations for how to strengthen the U.S. electrical grid. One simple fix to increase the physical integrity is to protect critical components with multiple barrier layers consisting of defensive fencing, video monitoring, and hardened walls to protect against easy access and external line-of-sight threats. This would help to keep out low-level threats and defend against easily-acquired threat weapons, such as high-powered rifles. This may not deter a significant state-level adversary with strong motivations, training and support, but may provide enough complications to terrorists and anti-government individuals to deter their decision for this avenue of attack.

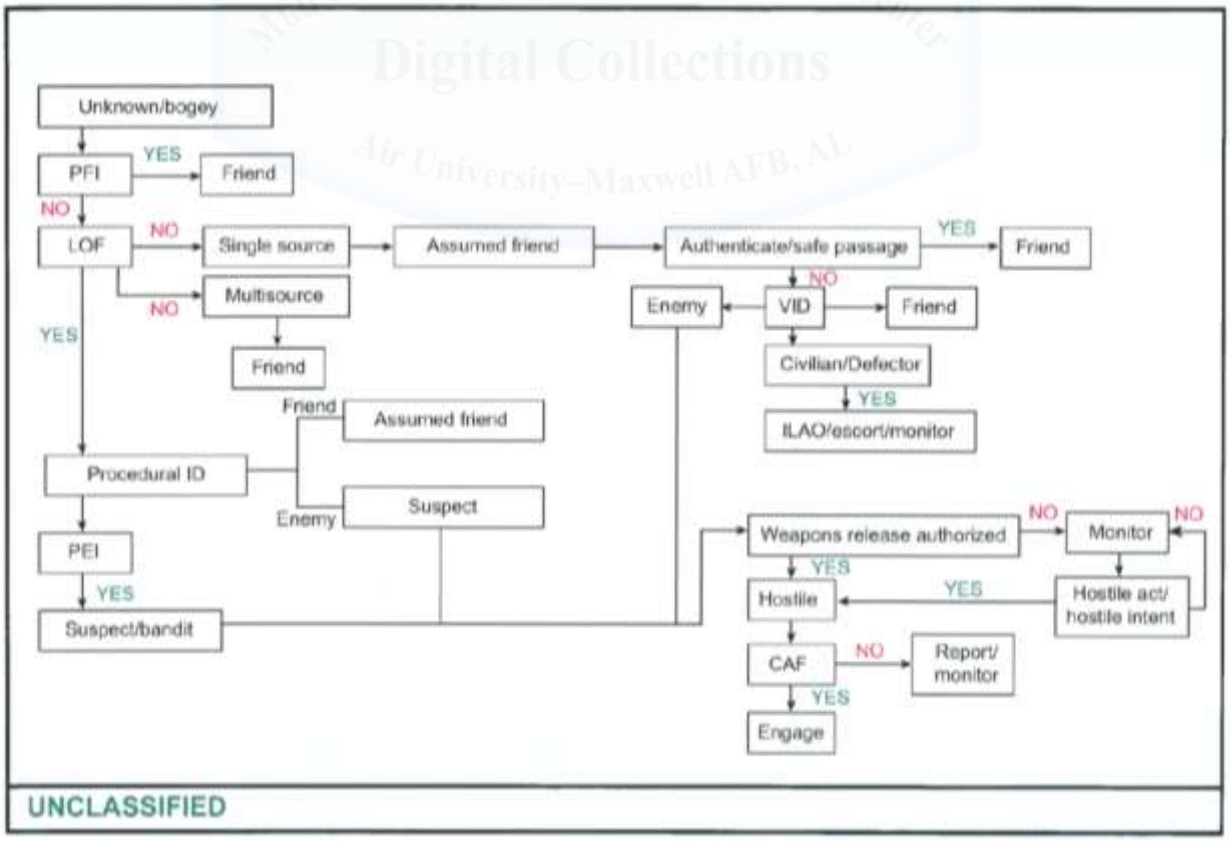
Other measures that could have significant impacts in protecting the grid components from malicious cyberattacks involve advanced training of individuals having access to C2 architecture as well as information-technology support personnel. Some of these improvements may be elementary-level protections, yet studies have shown they are often the weakest links - and subsequently easiest intrusion points - for adversaries to exploit. Suggestions for these range from simple account and password encryption, changing default passwords and accounts from the manufacturer, requiring complex passwords, removing unused services from computers, keeping patches up to date, and setting permissions for file access.[65] Information sharing between DoD and private energy industries could also stand to reap significant benefits by alerting the hundreds of energy companies to known threats and vulnerabilities that could impact their network's security. As of now, there is little communication and cooperation between private companies and the government, in part because companies fear a public perception of unreliable power delivery.

International Coalition / Task Force on Cyber Policing

One of the primary difficulties of extending deterrence to the cyber domain is attribution of hostile actions on the correct threat actor as well as having the will or jurisdiction to enact punishment against the actors. In establishing an international coalition to attack these problems, the U.S. should consider that "international threats require international solutions" to generate international stage legitimacy, support through manpower and information-sharing capabilities from various proprietary technologies.[66] Another reason for such a coalition construct is that - in order to create deterrence in a domain such as cyber - the international community needs to create and establish a "shared framework for judging how...cyberattacks correspond with interactions with other domains and...with political relations between potential adversaries during peacetime, in crises, and in wars."[67] One such international construct that offers a starting point is NATO, which could offer "a venue in which threat-related information may be shared" as well as "cyber defense efforts" in order to protect the overall health of the international community.[68] By engaging in a coalition-style effort, the U.S. can contribute to shaping the international norms of cyber behavior by having the legitimacy of international backing and a policing force to help establish the boundaries of this newest domain of operations and warfare.

Decision Matrix and Communication Architecture

The majority of open-source research concludes that cyberattacks go largely unpunished due to a seeming lack of consensus on pre-determined response options as well as a clearly established communication network between civilian electricity suppliers and government agencies that have the capability to help provide defense. With that problem in mind, this paper's final proposal will use the familiar air battle tools of the Identification (ID) Matrix and Rules of Engagement (ROE) – used by combatants to determine if they are allowed to preemptively engage a threat, monitor for further ID, or reactively strike back in retaliation or self-defense – as a departure point to offer a solution that enables swift, credible and predictable U.S. responses to cyberattacks on our critical infrastructure. Successively, this will help generate deterrence of future conflict in the cyber domain.



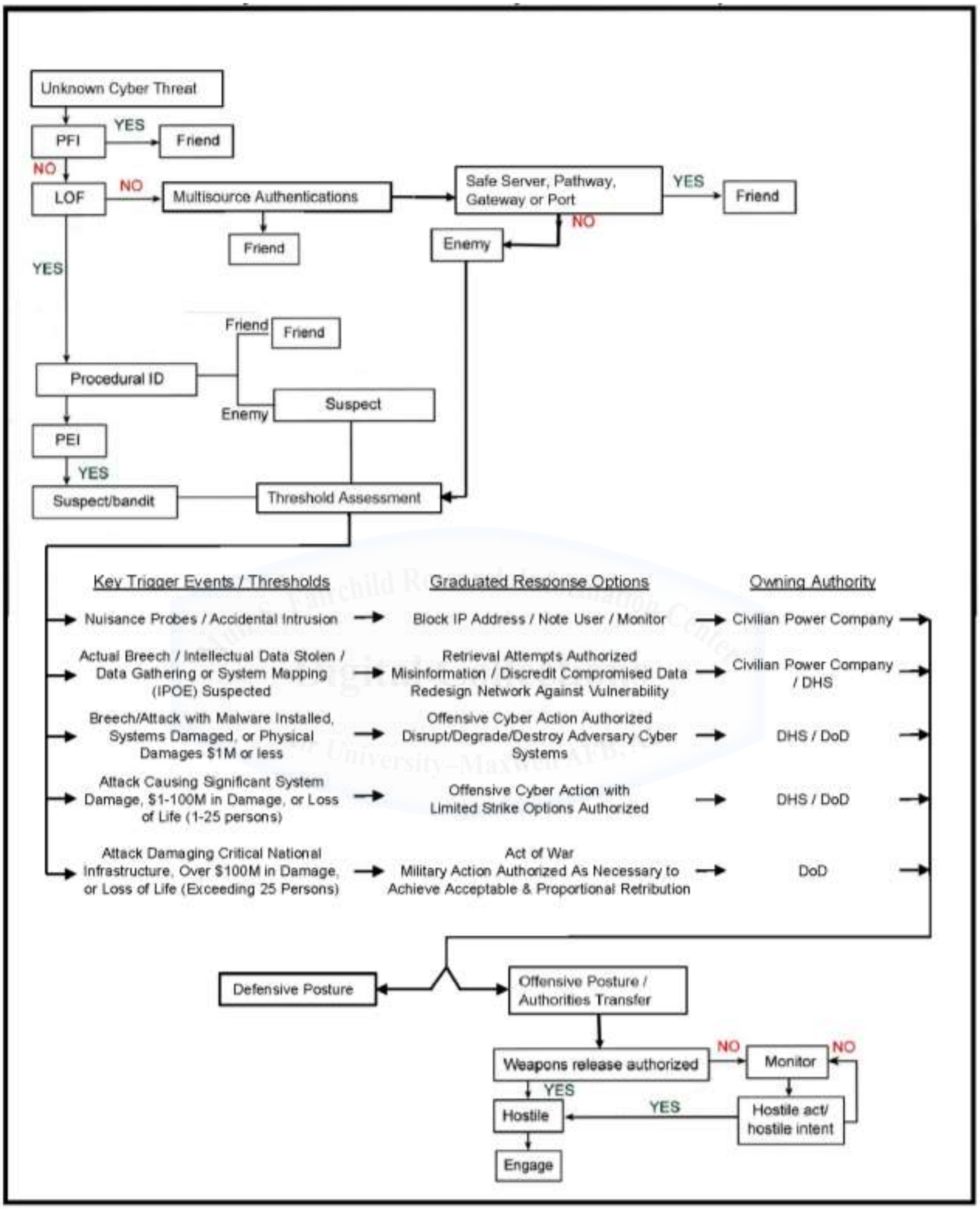
Air-to-Air ID-ROE Matrix Example[69]

The above Air-to-Air ID-ROE Matrix is currently in use by Air Force C2 platforms and fighter aircrew to quickly determine if unknown contacts entering a theater of operations 1) are friendly, neutral or enemy aircraft, 2) pose a threat to U.S. forces, and 3) satisfy ROE requirements to engage and neutralize. The following pertinent definitions will explain each aspect. Positive Identification (PID), labeled here as Friend (PFI) or Enemy (PEI) is "the unambiguous label...given to contacts identified from combat identification systems." [70] Another term used is Combat Identification (CID), or "the process of attaining an accurate characterization of detected objects in the operational environment sufficient to support an engagement decision."[71] Procedural Identification, "determined by track origination and behavior (including) point of origin (POO)," is used to determine where the aircraft originated from and if it is adhering to established theater instructions on where to fly, how to transit the airspace, what altitudes to fly at, and if it is transmitting the correct Identification Friend or Foe (IFF) code.[72] Lack of Friendly (LOF) is applied if the aircraft "lacks all modes/codes as required by local ROE" and serves to rule out the possibility of engaging friendly forces.[73] Positive Enemy Indications (PEI) are "unambiguous indications that a track/target is an enemy aircraft" and may be derived from electronic ID (EID) or visually acquired (VID).[74] Additionally, Hostile Act (HA) and Hostile Intent (HI) are "an attack or other use of force against the United States," or the threat thereof, and can be applied to "US nationals, their property (or) US commercial assets."[75] Clear Avenue of Fire (CAF) is a last check to ensure no friendly forces are in the line of fire. Finally, Guilt by association (GBA) criteria – the "process of identifying an entire formation…based on the identification of at least one member of that formation" – can be useful in the cyber realm to tie collaborating parties together.[76] Combining this into a formula helps combatants quickly and decisively engage or rule-out potential threats:

PID/CID/PEI/POO/GBA + LOF + HA/HI + CAF = Cleared to Engage IAW Theater ROE

Applying this formula to the problem at hand, we can create a similar decision and authority matrix to help cyber defenders facilitate real-time decisions against threat actors attacking U.S. infrastructure networks.

In order to create a new decision matrix for the cyber domain, a few assumptions need to be established to understand the logic behind its structure. These may change during the development of a real and working matrix for future cyber defense operations. First, the matrix assumes a defensive posture, established to protect a known system (i.e. electrical grid) in which defenders patrol for abnormalities. Second, the defenders are able to observe issues in real or near real-time, which reflects a future posture of persistent cyber presence. Third, it is assumed that an adversary *will* get into the network and it is only a matter of when. Fourth, the cyber realm is treated as a domain that needs protection – as much as air, land or sea domains – and not a supporting infrastructure, which compels a greater level of protection and response. Fifth, the communication and networking architecture is presumed to be engineered and enables a seamless transfer of controls between civilian, government and military entities (i.e. power companies to DHS to DoD). Finally, the dollar amounts and loss-of-life numbers are illustrative of the kinds of thresholds that government leaders need to establish, but are not expected to be a published (or unclassified) value. In addition to provoking public outcry for "allowing" a loss of human lives, it would create a known threshold for adversaries to test, or aim under, in order to preclude state response. Vague and subjective terms such as "moderate," "significant" and "extreme" should suffice to keep U.S. responses open to interpretation and deterrent in nature.



Key Trigger Events / Thresholds	Graduated Response Options	Owning Authority
Nuisance Probes / Accidental Intrusion	Block IP Address / Note User / Monitor	Civilian Power Company
Actual Breech / Intellectual Data Stolen / Data Gathering or System Mapping (IPOE) Suspected	Retrieval Attempts Authorized Misinformation / Discredit Compromised Data Redesign Network Against Vulnerability	Civilian Power Company / DHS
Breech/Attack with Malware Installed, Systems Damaged, or Physical Damages $1M or less	Offensive Cyber Action Authorized Disrupt/Degrade/Destroy Adversary Cyber Systems	DHS / DoD
Attack Causing Significant System Damage, $1-100M in Damage, or Loss of Life (1-25 persons)	Offensive Cyber Action with Limited Strike Options Authorized	DHS / DoD
Attack Damaging Critical National Infrastructure, Over $100M in Damage, or Loss of Life (Exceeding 25 Persons)	Act of War Military Action Authorized As Necessary to Achieve Acceptable & Proportional Retribution	DoD

Cyber Attack Decision Authority-ID-ROE Matrix Example

Working term definitions in the proposed Decision Authority-ID-ROE matrix are similar to the Air-to-Air matrix. Positive friendly ID can be established through observable defenses, pre-determined protocols and authentication measures to identify authorized personnel working on or maintaining systems. LOF indications trigger multisource authentication, such as cross-checking the behavior as well as gateways, ports and servers being used. If neither of these indicates a friendly source, cyber defenders can start to search for PEI or apply the criteria of GBA, POO and CID to identify a hostile actor.

After identifying a threat actor, pre-determined thresholds and trigger events will be referenced to authorize graduated response measures proportional to the level of attack. As an example, these actions may start with simple defensive measures for nuisance and accidental network probes; ramp up to retrieval and misinformation campaigns for a breech resulting in data theft; escalate to offensive cyber operations to disrupt, degrade or destroy adversary cyber systems; further escalate to limited strike options for attacks of significant damage; and, finally, culminate in a declaration of war that warrants full usage of military action. Throughout the decision process, assessment of an adversary's Hostile Act or Hostile Intent will be considered as means to accelerate the timeline or skip ahead to the threshold determination if imminent danger is encountered or suspected – similar in concept and criteria to that of self-defense. Clear Avenue of Fire has been removed from the current cyber example, but warrants further assessment to determine if unintended "civilian casualties" from certain cyber responses exist, and where its equivalent step should be placed along the matrix timeline.

Assuming the communication architecture between civilian and military authorities is already in place, it is also important to address the necessity. When civilian agencies are attacked, there is seldom a call for government help – through the Department of Homeland

Security (DHS) or Department of Defense (DoD) – or it occurs long after the fact, where the chance to intercept or disrupt the attack is far too late. If cyber defenders across the U.S. are able to tie into C2 architecture, both civilian and military entities could benefit from the information-sharing and team efforts to combat intrusion. Having military channels integrated would also allow transfer of defensive control to the DoD when an attack becomes too challenging for non-military grade equipment to counter. Many variables will have to be resolved beforehand, as the military cannot perform full-time security for every networked corporation, but if the cooperative architecture can be successfully integrated, a united defensive effort will provide much greater deterrence to future adversaries.[77]

Finally, after establishing a matrix for ID and ROE decisions, the U.S. needs to ensure "that those charged with securing critical infrastructure have the necessary authorities, information, and capabilities" delegated down to them.[78] Following this, a broadcast of U.S. intentions with regard to protecting cyber-security interests "must be clearly written," leaving an adversary with no doubt about "what the consequences will be if the red lines are crossed."[79] This final step will let the international community know where the U.S. stands on protecting its infrastructure and is a critical aspect for rebuilding deterrence.

Analysis

Physical protections, hardware and software upgrades, and increased training would all have considerable and immediate benefits for the protection of the physical grid network. In addition, implementation of the security protocols highlighted throughout various studies will benefit deterrence by reducing the easy access resulting from common human tendencies of habit and laziness.

An international coalition or task force would benefit partner nations by integrating the latest defensive technologies and allow open collaboration and information-sharing in order to target and deter hostile cyber actors. In practice, however, the benefits of such a coalition will be difficult to achieve. Information-sharing is often restricted because countries understandably limit the release of proprietary knowledge and capabilities to ensure they don't become negated through compromise. Further, the ideal intentions behind coalitions such as NATO have shown a consistent lack of perseverance when actions are necessary; it is challenging, at best, to get unanimous agreement and support from numerous and diverse nations.

Making efforts to establish a Decision Authority-ID-ROE matrix now would lay the groundwork for more persistent cyber operations in the future; "if the United States is to shape the development of international cyberspace norms, (it can only be done) through active cyber operations that begin to shape the parameters of acceptable behavior."[80] This proactive stance to curb threats before they get out of hand is an active deterrence measure that may prove far more beneficial than the passive and noncommittal "operational restraint" currently in place. As Fischerkeller states, "a doctrine of active mitigation may (actually) be less escalatory than one of restraint."[81] Put another way, it is always better and easier to address an issue as soon as possible, such as through persistent engagement. If the U.S. continues to operate under restraint, then it must always wait until an attack or resulting damage becomes so severe that it finally warrants response. This is directly responsible for creating the current permissive environment, in which adversaries continually probe all available avenues of access until deterrence and retaliation measures are enforced. Until then, they will remain under the U.S. response threshold, yet they still gain access to valuable U.S. property and infrastructure, inflicting considerable financial and economic damage on U.S. citizens.

The Decision Authority-ID-ROE matrix stands the best chance of success for cyber deterrence because it changes America's posture from operational restraint to that of cyber persistence, while working to improve communication and interaction between civilian, DHS and DoD entities. Further, information-sharing has the benefit of creating an "expert forum" where the brightest cyber minds can work together to tackle the responsibility of securing national infrastructure and interests. Agreeing upon and establishing this matrix construct forces national leadership to develop pre-determined thresholds and response criteria so that defenders and operators are unhindered in their mission execution. In addition, disseminating authorities down to the lowest acceptable and appropriate level increases the effectiveness of cyber operators by giving them responsibility and trust to carry out their tasks. Finally, implementing the Decision Authority-ID-ROE matrix is an important first step towards proactive engagement and norms development for a future world dominated by the cyber domain and enabled by its connectivity.

Recommendations

The quintessential recommendation is to implement all the proposed courses of action, simultaneously and to the fullest extent. A more realistic expectation is to tackle the problem in three phases. First, immediately implement upgrades to the most critical nodes and components of the electrical grid to ensure their survivability from all threats, physical and cyber. Second, develop a comprehensive matrix of thresholds, responses, decision authorities, and communication-integration policies to ensure a layered defense network for not just the electrical grid, but all critical U.S. infrastructures. Third, make the matrix and cooperation effort a model example for other countries to follow; encourage coalition participation for a unified effort to combat infrastructure and cyber intrusions or attack. Finally, thoroughly communicate the plan to educate the American public about the necessities and efforts as well as self-protection measures people can take. In turn, communicate the message of U.S. resolve to combat any attack effort taken on its national electric grid.

Conclusion

In conclusion, the U.S. electrical grid has both inherent vulnerabilities and robustness. Taking advantage of the redundancy and diversity of equipment, and then seizing the opportunity to upgrade known weaknesses can create significantly greater obstacles for future adversaries who wish to target the grid. Physical enhancements can secure critical equipment nodes and protect from low-level armed attack as well as higher level EMP/DEW attempts. International or coalition cyber-policing efforts can streamline information-sharing, minimize redundant workload and increase legitimacy when prosecuting external threat actors. Finally, adoption of a Decision Authority-ID-ROE matrix could strengthen future U.S. deterrence by enabling a posture of cyber persistence and delivering retribution to actors who wish to challenge U.S. resolve to protect its critical electrical grid infrastructure.

Notes

[1] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, U.S. Department of Energy: Office of Energy Policy and Systems Analysis (EPSA), August 2016, 21.

[2] Donald J. Trump, *The National Security Strategy of The United States of America*, Washington, DC: Joint Chiefs of Staff, December 2017, 13.

[3] Ibid, p.27.

[4] U.S. Energy Information Administration, “Electricity Explained: How Electricity is Delivered to Consumers,” *EIA.gov*, Washington, DC, 31 August 2017. https://www.eia.gov/energyexplained/index.cfm?page=electricity_delivery.

[5] Will R. Daugherty, “Lloyd’s Report Highlights Risk of Cyberattacks on National Power Grid,” *Data Privacy Monitor*, (Houston, TX: BakerHostetler, 23 July 2015), https://www.dataprivacymonitor.com/cybersecurity/lloyds-report-highlights-risk-of-cyberattacks-on-national-power-grid/.

Notes

[6] Clark W. Gellings and Kurt E. Yeager, "Transforming the Electric Infrastructure," *Physics Today* 57, no. 12 (December 2004), 49.

[7] Thomas F. McLarty III and Thomas J. Ridge, "Securing the U.S. Electrical Grid," *Center for the Study of the Presidency & Congress,* (Washington, DC, October 2014), 1.

[8] Peter Behr, "Substation Attack is New Evidence of Grid Vulnerability," *Energywire,* Washington, DC, 06 October 2016, https://www.eenews.net/stories/1060043920.

[9] Idaho National Laboratory, *Cyber Threat*, 21.

[10] Ibid, 21.

[11] Robert K. Knake, *A Cyberattack on the U.S. Power Grid*: *Contingency Planning Memorandum No. 31*. New York, NY: Council on Foreign Relations, April 2017, 4.

[12] Ibid, 5.

[13] Ibid, 4.

[14] Stefan Frei, *Vulnerability Threat Trends: A Decade in Review, Transition on the Way,* NSS Labs Analyst Brief (Austin, TX: NSS Labs, 2013), 1.

[15] Ibid, 7.

[16] Raymond K. Fink, David F. Spencer, and Rita A. Wells, *Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems*, National SCADA Test Bed (Washington, DC: U.S. Department of Energy, September 2006), 12.

[17] Zalmay Khalilzad, *Defense in a Wired World: Protection, Deterrence, and Prevention,* RAND Report – Strategic Appraisal: The Changing Role of Information in Warfare, Ch. 14 (Santa Monica, CA: RAND, 1999), 404.

[18] Khalilzad, *Defense in a Wired World*, 418.

[19] James R. Clapper, *Worldwide Cyber Threats*, Statement for the Record (Washington, DC: House Permanent Select Committee on Intelligence, September 2015), 2-3.

[20] Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid*, Lloyd's Emerging Risk Report (Cambridge, UK: Cambridge Centre for Risk Studies, May 2015), 55.

[21] Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?" Joint Force Quarterly 66 (3rd Quarter 2012), 10.

[22] Ibid, 10.

[23] Ibid, 11.

[24] Frank J. Cilluffo and Sharon L. Cardash, "Cyber Domain Conflict in the 21st Century," *The Whitehead Journal of Diplomacy and International Relations* 14, no 1 (Winter 2013), 44.

[25] Kenneth Geers, "The Challenge of Cyber Attack Deterrence," *Computer Law & Security Review* 26 (2010), 299.

[26] Jacquelyn Schneider, "Cyber and Cross Domain Deterrence: Deterring Within and From Cyberspace," (Draft Chapter for) *Cross-Domain Deterrence: Strategy in an Era of Complexity*, eds. Erik Gartzke and Jon Lindsay, Oxford University Press, 5.

[27] Ibid, 6.

[28] Ibid, 13.

[29] Michael P. Fischerkeller and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis*, Summer 2017, 382.

[30] Ibid, 382.

[31] Ibid, 388.

Notes

[32] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01A, *Standing Rules of Engagement for US Forces*, 15 January 2000, 1.
[33] Gellings and Yeager, “Transforming the Electric Infrastructure,” 45.
[34] Ibid, 46.
[35] Ibid, 45-46.
[36] Ibid, 46.
[37] EIA, “Electricity Explained.”
[38] Ibid.
[39] Ibid.
[40] Gellings and Yeager, “Transforming,” 48.
[41] Shane Harris, “‘Military-Style’ Raid on California Power Station Spooks U.S.,” *foreignpolicy.com*, 27 December 2013, http://complex.foreignpolicy.com/posts/2013/12/24/power-station-military-assault.
[42] Behr, “Substation Attack.”
[43] Behr, “Substation Attack.”
[44] Fink, Spencer and Wells, *Lessons Learned*, 1.
[45] Khalilzad, *Defense in a Wired World*, 404.
[46] Centre for Risk Studies, *Business Blackout*, 50.
[47] McLarty and Ridge, “Securing the U.S. Electrical Grid,” 14.
[48] Clapper, *Worldwide Cyber Threats*, 3.
[49] McLarty and Ridge, “Securing the U.S. Electrical Grid,” 21.
[50] Frei, *Vulnerability Threat Trends*, 10.
[51] Ibid, 1.
[52] Daugherty, “Lloyd’s Report Highlights Risk.”
[53] Cilluffo and Cardash, “Cyber Domain Conflict,” 42.
[54] Ibid, 41.
[55] Gellings and Yeager, “Transforming,” 49.
[56] Cilluffo and Cardash, “Cyber Domain Conflict,” 43.
[57] Clapper, *Worldwide Cyber Threats*, 3.
[58] Gellings and Yeager, “Transforming,” 49.
[59] Trump, *National Security Strategy*, 12.
[60] Geers, “Challenge of Cyber Attack Deterrence,” 302.
[61] Clapper, *Worldwide Cyber Threats*, 4.
[62] Manzo, *Deterrence and Escalation*, 10.
[63] Fisherkeller and Harknett, “Deterrence is Not a Credible Strategy,” 386.
[64] Clapper, *Worldwide Cyber Threats*, 3.
[65] Fink, Spencer &Wells, *Lessons Learned from SCADA Assessments*, 7-10.
[66] Cilluffo and Cardash, “Cyber Domain Conflict,” 45.
[67] Manzo, *Deterrence and Escalation*, 11.
[68] Cilluffo and Cardash, “Cyber Domain Conflict,” 45.
[69] Air Force Tactics, Techniques, and Procedures (AFTTP) 3-1.General Planning, Attachment 2. *Air-to-Air and Air-to-Ground Identification Criteria and Rules of Engagement Considerations*. 11 January 2016, A2-5. (releasable per ACC/A3, 1 Jun 18)
[70] Ibid, A2-1.

Notes

[71] Ibid, A2-1.
[72] Ibid, A2-1.
[73] Ibid, A2-2.
[74] Ibid, A2-2.
[75] CJCSI 3121.01A, *Standing ROE*, 2013, A-12.
[76] AFTTP 3-1.GP Att 2, A2-3.
[77] Trump, *National Security Strategy*, 32.
[78] Ibid, 13.
[79] Geers, "Challenge of Cyber Attack Deterrence," 302.
[80] Fisherkeller and Harknett, "Deterrence is Not a Credible Strategy," 382.
[81] Ibid, 382.

BIBLIOGRAPHY

Air Force Tactics, Techniques, and Procedures (AFTTP) 3-1.General Planning, Attachment 2. *Air-to-Air and Air-to-Ground Identification Criteria and Rules of Engagement Considerations*. 11 January 2016.

Behr, Peter. "Substation Attack is New Evidence of Grid Vulnerability." *Energywire*. Washington, DC (06 October 2016). https://www.eenews.net/stories/1060043920.

Centre for Risk Studies. *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid*. Lloyd's Emerging Risk Report. Cambridge, UK: Cambridge Centre for Risk Studies, May 2015.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01A. *Standing Rules of Engagement for US Forces*, 15 January 2000.

Cilluffo, Frank J., and Sharon L. Cardash. "Cyber Domain Conflict in the 21st Century." *The Whitehead Journal of Diplomacy and International Relations* 14, no. 1 (Winter 2013): 41-47.

Clapper, James R. *Worldwide Cyber Threats*. Statement for the Record. Washington, DC: House Permanent Select Committee on Intelligence, September 2015.

Daugherty, Will R. "Lloyd's Report Highlights Risk of Cyberattacks on National Power Grid." *Data Privacy Monitor*. Houston, TX: BakerHostetler, 23 July 2015. https://www.dataprivacymonitor.com/cybersecurity/lloyds-report-highlights-risk-of-cyberattacks-on-national-power-grid/.

Fink, Raymond K., David F. Spencer, and Rita A. Wells. *Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems*. National SCADA Test Bed. Washington, DC: U.S. Department of Energy, September 2006.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis*, Summer 2017: 381-393.

Frei, Stefan. *Vulnerability Threat Trends: A Decade in Review, Transition on the Way*. NSS Labs Analyst Brief. Austin, TX: NSS Labs, 2013.

Geers, Kenneth. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26 (2010): 298-303.

Gellings, Clark W., and Kurt E. Yeager. “Transforming the Electric Infrastructure.” *Physics Today* 57, no. 12 (December 2004): 45-51.

Harris, Shane. “‘Military-Style’ Raid on California Power Station Spooks U.S.” *foreignpolicy.com*. 27 December 2013. http://complex.foreignpolicy.com/posts/2013/12/24/power-station-military-assault.

Idaho National Laboratory. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*. U.S. Department of Energy: Office of Energy Policy and Systems Analysis (EPSA), August 2016.

Khalilzad, Zalmay. *Defense in a Wired World: Protection, Deterrence, and Prevention.* RAND Report – Strategic Appraisal: The Changing Role of Information in Warfare, Ch. 14. Santa Monica, CA: RAND, 1999, 403-437.

Knake, Robert K., *A Cyberattack on the U.S. Power Grid: Contingency Planning Memorandum No. 31*. New York, NY: Council on Foreign Relations. April 2017.

Manzo, Vincent. “Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?” *Joint Force Quarterly* 66 (3rd Quarter 2012): 8-14.

Mattis, James N. *The National Defense Strategy of The United States of America*. Washington, DC: Joint Chiefs of Staff, January 2018.

McLarty, Thomas F., III and Thomas J. Ridge. “Securing the U.S. Electrical Grid.” *Center for the Study of the Presidency & Congress.* Washington, DC, October 2014.

Schneider, Jacquelyn. “Cyber and Cross Domain Deterrence: Deterring Within and From Cyberspace,” (Draft Chapter for) *Cross-Domain Deterrence: Strategy in an Era of Complexity*, eds. Erik Gartzke and Jon Lindsay, Oxford University Press.

Trump, Donald J. *The National Security Strategy of The United States of America*. Washington, DC: Joint Chiefs of Staff, December 2017.

U.S. Department of Energy. “Grid Modernization and the Smart Grid.” *Energy.gov*. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid.

U.S. Energy Information Administration. “Electricity Explained: How Electricity is Delivered to Consumers.” *EIA.gov*. Washington, DC, 31 August 2017. https://www.eia.gov/energyexplained/index.cfm?page=electricity_delivery.