ANU NARAYANAN, JONATHAN WILLIAM WELBURN,
BENJAMIN M. MILLER, SHENG TAO LI, AARON CLARK-GINSBERG

Deterring Attacks Against the Power Grid

Two Approaches for the U.S. Department of Defense

For more information on this publication, visit www.rand.org/t/RR3187

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0416-9

Published by the RAND Corporation, Santa Monica, Calif.

Cover: kosssmosss - stock.adobe.com

Preface

The U.S. Department of Defense (DoD) increasingly relies on electric power to accomplish critical missions. As a result, ensuring that forces and facilities have access to a reliable supply of electric power is critical for mission assurance. However, DoD does not directly manage its supply of power; most of the electricity consumed by military installations in the continental United States comes from the commercial grid—a system that is largely outside of DoD control and increasingly vulnerable to both natural hazards and deliberate attacks. DoD already undertakes activities to improve mission resilience to grid outages for systems or infrastructure that it does manage or control, but it could benefit from further considerations of where, when, and how to pursue various methods for boosting the power resilience of systems or infrastructure outside its control. This study examines two approaches that DoD might consider as options for deterring attacks against the power grid.

RAND Ventures

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND Ventures is a vehicle for investing in policy solutions. Philanthropic contributions support our ability to take the long view, tackle tough and often-controversial topics, and share our findings

in innovative and compelling ways. RAND's research findings and recommendations are based on data and evidence and therefore do not necessarily reflect the policy preferences or interests of its clients, donors, or supporters.

Funding for this venture was made possible by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

Contents

Figures and Tables

Figures

Tables

Summary

The rapid pace of technological change has touched nearly every facet of life in the United States, and armed conflict is no exception. Increased reliance on intelligence processing, exploitation, and dissemination; networked real-time communications for command and control; and a proliferation of electronic controls and sensors in military vehicles (such as remotely piloted aircraft), equipment, and facilities have greatly increased the U.S. Department of Defense (DoD)'s dependence on energy, particularly electric power, at installations. Although the power grid has long been susceptible to natural disasters, deliberate attacks, and the problems of aging infrastructure, its vulnerability to attacks is increasing (Nicholson et al., 2012; Zhu, Joseph, and Sastry, 2011). Paralleling technological advancement in vital mission support systems, the ability of adversaries to exploit vulnerabilities through cyber means has expanded, creating considerable risk to the stable supply of electric power.

Strictly preventive measures have been unable to completely eliminate threats to the electric power grid. Recent armed conflicts have seen both physical attacks and cyberattacks on electric power grids, but the problem has also affected other types of businesses and infrastructure. Despite guidance documents that press for the use of cybersecurity best practices across a range of industries, state actors have used cyber means to carry out notable attacks against numerous public institutions, private organizations, and individuals. Although threats to the power grid are by no means confined to state actors, many of these incidents have been attributed to nation-states. In this report, we focus on factors that deter actions by nation-states.

The accumulation of incidents despite efforts to bolster preventive measures has driven calls for a national policy on cyber deterrence. Congress has been one of the most ardent supporters of considering cyber deterrence, and it has used recent National Defense Authorization Acts to highlight the need for action. This report takes an initial step toward a framework to evaluate options for deterring cyberattacks on the power grid through denial and cost imposition. *Denial* is the strategy of removing the perceived benefits of an attack. *Cost imposition* is the threat of punitive measures to convince an adversary that the benefit of an attack might not be worth the cost; this might be the most widely employed deterrence strategy.

Deterrence by Denial

We first examine deterrence by denial. The intention of denial is to deter would-be adversaries from attacking, not necessarily because the ramifications of attacking are high but because even a successful attack would not accomplish the attacker's objectives.

There are multiple ways to deter cyberattacks on the power grid through denial. For instance, hardening the power grid in ways that reduce vulnerabilities and failure rates (i.e., increasing the reliability of the grid) can help ensure that the power sources upon which DoD relies are consistently able to provide the expected amount of power at any given point. Knowledge of such investments in the grid might, in turn, have a deterring effect by reducing or removing the perceived benefits that an adversary associates with an attack. Similarly, DoD could improve its mission resilience to successful cyberattacks on the power grid through investments in power resilience measures (e.g., backup power generators or DoD-owned primary or secondary power-generation sources).

In addition to providing value through deterrence of adversary attacks (cyber-related or otherwise), investments in measures aimed at limiting or denying adversary success serve a broader purpose of improving mission resilience to power disruptions resulting from natural disasters, operator error, or equipment failures.

In this report, we focus on *outside-the-fence* interventions—that is, interventions that involve improvements to systems or infrastructure that are not directly owned or managed by DoD. We identify three types of outside-the-fence interventions. The first category, *shifting the fence line*, includes any actions that change whether a specific aspect of the power grid (or other critical infrastructure system) is owned or operated by DoD or a non-DoD entity. The second category of outside-the-fence interventions, *influencing governance*, includes efforts to directly or indirectly influence how the electric power infrastructure system works, such as through directly or indirectly changing rules, regulations, or processes. The third category, *leveraging resources*, includes efforts to use money or other resources, such as land or people, to arrange or influence outside-the-fence outcomes.

We also aim to identify the contextual factors that influence the ease of implementing different types of outside-the-fence interventions. To this end, we examine how outside-the-fence options have been considered and applied in two case studies—one focused on water and the other on electric power. Supplementing insights gained from these case studies with literature reviews, we develop a framework that describes broad categories of outside-the-fence interventions that might be available to DoD in different settings, as well as the contextual factors that influence the ease of implementation of these options. Note that our intent is *not* to signal that outside-the-fence interventions are inherently preferred to inside-the-fence options. There are specific risks associated with outside-the-fence investments that would need to be weighed when making decisions about whether, how and where to make these investments. We also do not seek to recommend specific outside-the-fence interventions that DoD ought to implement. Ultimately, there is no one mix of inside- and outside-the-fence options that would work equally well across missions or installations. The right mix needs to be determined on a case-by-case basis. The proposed framework is meant to provide a conceptual structure upon which future discussions and analysis can be built.

Deterrence by Cost Imposition

In addition to deterrence by denial, U.S. cyber deterrence strategy includes deterrence by cost imposition. However, a lack of clarity in the application of international law and existing norms in cyberspace is a key challenge for understanding the available options for countering cyber aggression. We aim to elucidate potential options for deterring the threat of cyberattacks on the power grid through the threat of cost imposition, as guided by international law. Mainly, we provide a view of the bounds of international law as it pertains to cyber deterrence, particularly when it comes to deterring cyberattacks on the power grid.

Cyber Deterrence and International Law

International legal experts agree on general principles that govern retaliatory responses to cyberattacks on critical infrastructure, including the power grid. However, there remains disagreement about how these principles apply under specific circumstances, and the law continues to evolve based on these debates and on state practice.

Broadly speaking, international law requires retaliatory responses to be proportional to the hostile act. There are three general categories of retaliatory responses to cyberattacks: self-defense, countermeasures, and retorsions. The right of *self-defense* enables a state to use military force—which can include both cyber and kinetic operations—against an aggressor. Self-defense provides the most robust array of deterrence options and thus is available in response to only the most harmful types of cyber operations. When a state is subject to a cyberattack that falls short of an armed attack, it may not invoke the right to self-defense. But it may employ *countermeasures*, which are defined as otherwise unlawful acts that may be undertaken by an injured state in response to another state's intentionally wrongful conduct. The third category of retaliatory responses consists of *retorsions*, which are legally permissible but unfriendly acts.

The availability of each retaliatory response depends largely on two factors: the severity of the attack and the extent to which the attack may be attributed to a state. Retaliatory options are broadest when a state is the victim of a destructive or highly disruptive cyberattack that

is attributable to another state. Conversely, options are most narrow when a cyber operation produces little or no physical consequences or is launched by a nonstate actor that has limited connection to a state.

Table S.1 maps the aforementioned retaliatory options. The vertical categories from top to bottom represent the objects of attribution: a state actor, a nonstate actor under state control or direction, and a nonstate actor with little or no state support. Although the legal attribution need not be foolproof, it must be based on reasonable evidence. The technical challenges of cyberattack attribution could inhibit the ability to retaliate. The horizontal categories in Table S.1, from left to right, denote increasing severity of the cyberattack:

- an unlawful intervention (less than use of force)
- a "less grave" use of force

Table S.1
Cost Imposition Options

	Severity (Intended or Actual) →		
Attributed Actor	**Less Than Use of Force**	**Use of Force**	**Armed Attack**
State actor	Nonforceful countermeasures (including cyber counterattacks)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks)	Use of force in self-defense against the state
Nonstate actor under state control or direction	Nonforceful countermeasures (including cyber counterattacks targeting the state or nonstate actor)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks targeting the state or nonstate actor)	Use of force in self-defense against the state or nonstate actor
Nonstate actor with little or no state support	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Use of force in self-defense against the nonstate actor *only if* the host state is unwilling or unable to prevent attack

NOTE: In this table, we consider limited reprisals under the broad definition of deterrence.

- an armed attack (i.e., a "most grave" use of force) (see International Court of Justice, 2003).

Importantly, the "use of force" and "armed attack" thresholds remain ill-defined in the cyber context—and they are indeed incomplete even in the noncyber *jus ad bellum* framework. The United States therefore has discretion to advance its own definition within a space of reasonable debate.

Takeaways

In this report, we begin to develop options for using cost imposition measures to deter cyber aggression against the power grid. Although we use international law to guide the construction of these options, domestic law, regulations, and policy may further guide the options. However, we also find reason to believe that considerable uncertainty on cost imposition is likely. Efforts to ameliorate confusion may enhance the strength of deterrence by adding clarity to cost imposition. Although proposals to enhance attribution in cyberspace have been made, DoD efforts to strengthen credible attribution could work to enhance the cyber posture of the United States and the strength of deterrence. Furthermore, it may also work against deterrence to not have greater clarity on whether cyber aggression on the power grid carries the threat of legal countermeasures, cyber countermeasures, or the full force of the military. The solutions to each area of uncertainty are multifaceted and span matters of technology, law, policy, and strategy.

If adversaries believe that aggression will be followed by only low-level cost imposition, deterrence could be undermined. Perhaps worse, uncertainty could lead to unintended escalation. In the case of Russian aggression against the U.S. power grid, the United States might interpret Russian movements in cyberspace as representative of an imminent attack while Russia views its own movements as routine espionage. It is therefore feasible that a cyberattack representing an imminent use of force could be responded to with a military strike using kinetic force, escalating the confrontation into a new domain.

Although aggression in the cyber domain presents new challenges for international law and thus deterrence, options for cost imposition remain the same. Depending on the adversary and the severity of the attack, the U.S. government and DoD will face the decision of how to respond—with or without force, within the cyber domain or not. The options presented in this discussion can aid DoD in articulating the threat of cost imposition.

Conclusion

This report explores two approaches for deterring attacks against the U.S. power grid in a world of increasing cyber aggression: enhancing resilience and reliability to deter by denial and using the threat of retaliation to deter by cost imposition. The report is a first step, exploring how both approaches lead to options for inclusion in a broader deterrence strategy. These two approaches are not substitutes; they are complementary to each other and to other defense strategies.

For deterrence by denial, we lay the groundwork for how DoD might identify and compare options for improving mission resilience through investments in outside-the-fence interventions. Improving resilience and reliability can enhance DoD's ability not only to deter attacks by a military adversary but also to sustain operations under a broader set of potential perils, such as natural disasters, aging infrastructure, and other types of intentional harm to the power grid.

By exploring the applicability of international agreements on the law of war, we discuss options for deterring cyberattacks through the threat of cost imposition. For cyberattacks on the civilian electric power grid, we find that the severity of the attack and the strength of attribution reveal several options for retaliation. However, one challenge for deterrence comes from the ambiguity of cyberspace. We find that this ambiguity cuts in two key directions: cyberattack attribution and cyberattack severity. The problem of attribution is well known: It leads to unavoidable challenges in retaliating against attacks and, as a result, risks undermining deterrence. The ambiguity surrounding severity may lead to less-obvious problems; we find reason for concern

that a lack of clarity on the meaning of use of force in cyberspace could produce unintended escalation. That is, cyber activity on the power grid that fits well within one country's definition of espionage could be interpreted by another country as an imminent attack leading to military retaliation and unintended escalation.

The exploration of deterrence options in this report opens several questions for future work. For example, future analyses could further explore the optimality of different resilience strategies and their contributions to deterrence by denial. Similarly, future analyses could evaluate the strategic benefit of the deterrence by cost imposition options discussed in this report.

Acknowledgments

This project was funded, in part, through RAND's program of self-initiated research. We are grateful to Howard Shatz, Obaid Younossi, and Ted Harshberger for their leadership and support and to King Mallory and Burgess Laird for their critical reviews of earlier drafts. We also thank Anita Szafran for her thorough pursuit of supporting data, as well as Jacob DeWeese for his excellent research assistance. We thank Laurel Miller for providing insightful and helpful guidance early on, Naomi Hale for her administrative assistance, and Allison Kerns for carefully editing the final version of the report. In the end, the authors are wholly responsible for any errors and omissions that remain.

Abbreviations

ACD	Armed Conflict Database
AFB	Air Force Base
AFRI	Air Force Research Institute
AWWA	American Water Works Association
CFR	Council on Foreign Relations
CSIS	Center for Strategic and International Studies
DoD	U.S. Department of Defense
EMP	electromagnetic pulse
FAR	Federal Acquisition Regulation
FY	fiscal year
ICJ	International Court of Justice
IGSA	intergovernmental support agreement
IISS	International Institute for Strategic Studies
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
OG&E	Oklahoma Gas and Electric
PWC	Public Works Commission
THOR	Theater History of Operations
US-CERT	U.S. Computer Emergency Readiness Team
WaterISAC	Water Information Sharing and Analysis Center

CHAPTER ONE

Introduction

The rapid pace of technological change has touched nearly every facet of life in the United States, and armed conflict is no exception. Increased reliance on intelligence processing, exploitation, and dissemination; networked real-time communications for command and control; and a proliferation of electronic controls and sensors in military vehicles (such as remotely piloted aircraft), equipment, and facilities have greatly increased the U.S. Department of Defense (DoD)'s dependence on energy, particularly electric power, at installations. The fact that most electricity consumed by DoD installations in the continental United States is drawn from the commercial electric power grid (henceforth referred to as the *power grid*) underscores the significance of DoD's reliance on that power grid.[1] Although the power grid has long been susceptible to natural disasters, deliberate attacks, and the problems of aging infrastructure, its vulnerability to attacks is increasing (Nicholson et al., 2012; Zhu, Joseph, and Sastry, 2011). Paralleling technological advancement in vital mission support systems, the ability of adversaries to exploit vulnerabilities through cyber means has expanded, creating considerable risk to the stable supply of electric power.

On December 23, 2015, three Ukrainian regional power distribution companies went offline, taking down substations and shutting off power for 230,000 of their customers (Industrial Control Systems Cyber Emergency Response Team, 2018; Zetter, 2016). The outage

[1] We focus on installations in the continental United States, but the general ideas presented in this report can be extended, with modifications, to settings outside that area.

was no accident. Russian state actors had illegally accessed the company networks, performed months of reconnaissance, and eventually took control of the supervisory control and data acquisition systems in a coordinated cyberattack (Greenberg, 2017a). Although operators were able to manually restore power within approximately six hours, the damage inflicted from wiping systems and destroying compromised devices left Ukrainian operators without automated control of power distribution for about a year (Dragos, 2017). And the threat is far from over. In the years since, teams of Russian hackers have successfully disrupted the Ukrainian electric grid through cyber means, notably in December 2016 and June 2017 (Dragos, 2017).

Unfortunately, Ukraine has not been the only target. On March 15, 2018, the U.S. Department of Homeland Security and the Federal Bureau of Investigation released a joint technical alert explaining an active cyber threat to the U.S. power grid (U.S. Computer Emergency Readiness Team [US-CERT], 2018). The public report revealed that the Russian government had engaged in cyber activities that targeted and compromised organizations and facilities operating the U.S. power grid dating back at least as far as March 2016 (US-CERT, 2018). With an increasingly real risk of adversary harm to the power grid, DoD should take its existing reliance on commercial power seriously.

In recent years, the services' leaders have recognized the gravity of this problem and increased their focus on energy assurance–related activities. As stated in DoD's 2012 mission assurance strategy,

> The Department of Defense's ability to ensure the performance of its Mission-Essential Functions (MEFs) is at growing risk. Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets . . . on which our forces depend. (DoD, 2012a, p. 1)

However, the question of whether DoD's current strategy for ensuring that electric power assurance is sufficient remains.

The Case for Deterrence

Strictly preventive measures have been unable to completely eliminate threats to the electric power grid. Recent armed conflicts have seen both physical attacks and cyberattacks on electric power grids, but the problem has also affected other types of businesses and infrastructure. In spite of guidance documents that press for the use of cybersecurity best practices across a variety of industries (e.g., National Institute of Standards and Technology [NIST], 2015; DoD, 2012b), state actors have used cyber means to carry out notable attacks against Sony Pictures; several U.S. banks; a New York dam; the U.S. Office of Personnel Management; the U.S. Department of State; the Democratic National Committee; and numerous other public institutions, private organizations, and individuals. Although many of these incidents have been attributed to nation-states, threats to the power grid are by no means confined to state actors. However, in this report, we focus on factors that deter actions by nation-states.

The accumulation of incidents despite efforts to bolster preventive measures has driven calls for a national policy on cyber deterrence. Congress has been one of the most ardent supporters of considering cyber deterrence, and it has used recent National Defense Authorization Acts (NDAAs) to highlight the need for action. For instance, Section 1636 of the NDAA for fiscal year (FY) 2019 states,

> It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests with the intent to [cause casualties, disrupt normal functioning, threaten the armed forces, or] achieve an effect . . . comparable to an armed attack. (Pub. L. 115-232, 2018)

The NDAA mentions that, to deter and respond to such attacks, the United States should evaluate options for military response, cost imposition, and denial. For denial specifically, Section 1636 states,

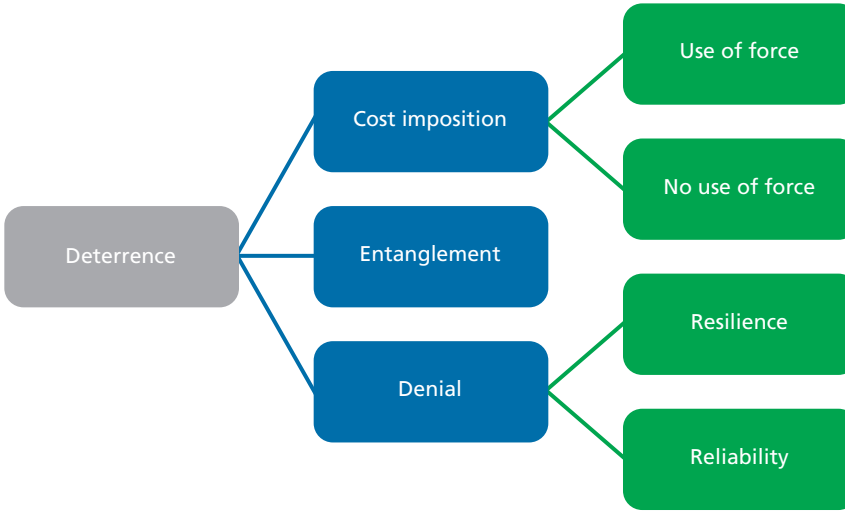
> the United States shall, to the greatest extent practicable, prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities described in subsection (a) of infrastructure critical to the political integrity, economic security, and national security of the United States. (Pub. L. 115-232, 2018)

Deterrence offers an alternative, complementary approach to addressing the failures of strictly defensive measures. *Deterrence* refers to the strategy of discouraging adversaries from attacking rather than limiting adversaries' ability to successfully attack. The theory is most widely known for the Cold War–era discussions of nuclear deterrence and mutually assured destruction (e.g., Schelling, 1981; Powell, 1990; Morrow, 1994) and hence was historically used in reference to physical events. Extending the theory to include cyberspace contexts introduces new challenges. Imperfect attribution and a lack of norms on cyber methods are two of the most pronounced challenges facing deterrence in cyberspace, and they have resulted in a lack of clarity on available deterrence options (Jasper, 2015; Nye, 2011). To understand potential options for deterring either physical attacks or cyberattacks, it is helpful to start with the three basic strategies of deterrence displayed in Figure 1.1: cost imposition, entanglement, and denial (Jasper, 2015; Nye, 2011; Schelling, 1981). This report takes an initial step in evaluating options for deterring cyberattacks on the power grid through cost imposition and denial.

Deterrence by Cost Imposition

The first path in the tree of deterrence options is cost imposition. The threat of punitive measures to convince an adversary that the benefit of an attack might not be worth the cost might be the most widely employed deterrence strategy. At a basic level, Americans routinely encounter this strategy in day-to-day life—for example, in the sign posted at the convenience store stating that "shoplifters will be punished" and the police officer on the side of the highway ready to pull

Figure 1.1
The Basic Strategies of Deterrence



over the next speeding driver. In each case, the threat of cost imposition is used to discourage individuals from carrying out an undesired action. The same is true for deterring military aggression. During the Cold War, second-strike capability in nuclear deterrence theory dissuaded adversaries from attacking by threatening that a successful nuclear strike would be met with a retaliatory nuclear strike (Powell, 1990).

Additionally, the tree in Figure 1.1 displays different paths for punishing an adversary by retaliation.[2] Retaliation can come in the form of either a use of force (e.g., a kinetic attack on a key adversary facility) or no use of force (e.g., economic sanctions). The potential options might be strategic (i.e., the use of force and the type of force pose trade-offs for deterrence efficacy and risk of escalation), as well as a matter of legal policy. In this report, we focus on the legal aspect and examine how international law, agreements, and norms bound DoD options for retaliation.

[2] We use the term *retaliation* throughout this report to mean the act of imposing a cost on an adversary in response to its unwanted actions.

Deterrence by Entanglement

The second approach to deterrence presented in Figure 1.1 is entanglement. Instead of relying on punitive measures, entanglement relies on the interconnections between the United States and potential adversaries to the point that any attack on the United States has immediate negative impacts for the attacker (Jasper, 2015). Economic entanglement, for example, could involve two economies that are heavily connected through trade such that a failure of the U.S. economy is guaranteed to negatively affect the potential adversary. This interdependence incentivizes each state to avoid an attack that might harm the other's economy.

For success, economic interdependency would need to be fostered by public (e.g., U.S. Department of Treasury, U.S. Department of State, U.S. Department of Commerce) and private organizations. Although the strategy goes beyond the purview of DoD, some have argued that it is a potential solution for active conflicts, including those with North Korea and various cyber actors (Jasper, 2015; C. Smith, 2006). Consequently, we acknowledge that entanglement should be considered by DoD in the portfolio of deterrence options; however, we limit our focus to areas in which DoD might develop deterrence strategies through denial and cost imposition.

Deterrence by Denial

Finally, Figure 1.1 displays a third path of deterrence: denial. Denial is the strategy of removing the actual or perceived benefits of an attack, in contrast to cost imposition and entanglement, which deter attacks through threat of harm to the attacker. One example of a denial strategy is when a taxi cab displays a sign that "drivers do not carry cash." If someone were to attempt to rob the taxi cab driver, he or she would be unable to receive any benefit from doing so. The intention of denial is to deter would-be adversaries from attacking, not necessarily because the ramifications of attacking are high but because even a successful attack would not accomplish the attacker's objectives.

There are multiple ways to deter cyberattacks on the power grid through denial. For instance, hardening the power grid in ways that reduce vulnerabilities and failure rates (i.e., increasing the *reliability*

of the grid) can help ensure that the power sources upon which DoD relies are consistently able to provide the expected amount of power at any given point. Knowledge of such investments in the grid might, in turn, have a deterring effect by reducing or removing the perceived benefits that an adversary associates with an attack.

Similarly, DoD could improve its mission resilience to successful cyberattacks on the power grid through investments in power resilience measures (e.g., backup power generators or DoD-owned primary or secondary power-generation sources) or other types of resilience measures (e.g., investments in continuity of operations plans that allow mission functions to be moved to other locations).[3] As with investments in grid reliability, an adversary with knowledge that such power resilience measures are in place might think twice before launching an attack on the grid specifically aimed at disrupting DoD operations.

In addition to providing value through deterrence of adversary attacks (cyber-related or otherwise), investments in measures aimed at limiting or denying adversary success serve a broader purpose of improving mission resilience to power disruptions resulting from natural disasters, operator error, or equipment failures.

Organization of This Report

The structure of the remainder of this report is as follows. Chapter Two focuses on deterrence by denial, identifying key factors that DoD might consider when working with non-DoD entities to support the reliability of DoD's electric power supply or to increase DoD's

[3] We define *resilience* as a system's ability to withstand and recover from a particular disruption (Narayanan et al., 2017). For some missions, resilience might mean never being offline; that is, to withstand a disruption might mean ensuring that operations are continuously sustained throughout the course of a disruption. For other missions, some amount of disruption might be acceptable. In addition, we distinguish between *mission* resilience and *power* resilience because mission resilience can be achieved in a variety of ways, not all of which involve investments in power resilience. Note that a closely related concept is *robustness*, which we define as DoD's ability to withstand and recover from a diverse set of disruptions (Narayanan, et al., 2017). Robustness can be thought of as the extent to which a system is resilient across a wide array of disruptions.

resilience to disruptions in power supply. Chapter Three focuses on deterrence by cost imposition, exploring international agreements on the law of war to elucidate potential punitive actions that could be used by deterrence strategy as it pertains to cyberattacks on the grid. Chapter Four presents our conclusions and identifies open questions.

CHAPTER TWO

Assessing Outside-the-Fence Options for Improving DoD Mission Resilience to Power Disruptions

Efforts to improve grid reliability and power resilience can reduce the likelihood of power-related disruptions to DoD missions. As discussed in the previous chapter, although making improvements to grid reliability and power resilience is not the sole method of deterring attacks on the power grid, it offers one way to deny, and thereby deter, such attacks. These improvements can be further broken down into two categories:

- Those that involve improvements to systems or infrastructure that are owned or managed by DoD. We refer to these as *inside-the-fence* interventions.
- Those that involve improvements to systems or infrastructure that are not directly owned or managed by DoD. We refer to these as *outside-the-fence* interventions.

This chapter provides guidance on how DoD might identify and implement beneficial outside-the-fence interventions. These interventions are distinct from inside-the-fence options for boosting DoD's electric power resilience, such as backup generators and uninterruptible power supply systems, which also play important roles in power resilience. The cost-benefit calculus for determining which inside-the-fence investments to make and when to make them involves (1) such complexities as scaling backup systems to match the critical load demanded over time and (2) uncertainties around the frequency and severity of outages (Narayanan et al., 2017). But this cost-benefit calculus is better understood than the cost-benefit calculus for determining the optimal

collection of outside-the-fence actions for DoD to pursue. Nevertheless, outside-the-fence engagement is an important tool that DoD can use to improve mission assurance through improving electric power resilience. Despite the lack of a systematic method for determining when and how DoD should engage in outside-the-fence actions to boost resilience, DoD has been increasingly experimenting with these forms of engagement for both resilience purposes and fiscal purposes. A large and growing literature documents collaborations between DoD and non-DoD entities that aim to improve the resilience of electric power and other utilities or services (Lachman et al., 2009; Lachman et al., 2011; Lachman, Resetar, and Camm, 2016; Lachman et al., 2016). Given the growing role of outside-the-fence options in DoD's toolkit for improving mission assurance, our goal in this chapter is to establish a baseline for how DoD might think about when, where, why, and how to increase outside-the-fence resilience.

Specifically, we seek to identify the contextual factors that influence the ease of implementing different methods of outside-the-fence interventions.[1] To this end, we examine how outside-the-fence options have been considered and applied in two case studies. We consider both electric power infrastructure and other similar infrastructure in order to include both outside-the-fence options that DoD is currently pursuing and those that it *could pursue* but has not yet. We neither develop a quantitative model for calculating the costs or benefits associated with different options nor recommend courses of action that DoD should take.

Furthermore, our intention is *not* to signal that outside-the-fence interventions are inherently preferred to inside-the-fence options.[2] We

---

[1] Implementation ease can be seen as one dimension of cost. Analyzing factors that influence the probability and magnitude of benefits is a separate and complex exercise that is saved for future work.

[2] Indeed, there are specific risks associated with outside-the-fence investments that would need to be weighed when making decisions about how and where to make these investments. The U.S. power grid is a public system that may not anticipate direct attack by an adversary state's military. The most recent kinetic attack by a state adversary was a largely ineffective Japanese submarine attack on the Ellwood oil installations on the Californian coast in 1942 (Reynolds, 1964). Today, there is increased concern about state-based adversaries attacking

also do not seek to recommend specific outside-the-fence interventions that DoD ought to implement. Ultimately, there is no one mix of inside- and outside-the-fence options that would work equally well across missions or installations. The right mix needs to be determined on a case-by-case basis. Regardless of whether the interventions in question fall inside or outside the fence line, selecting the right resilience options for a particular mission or installation should involve valuation exercises that begin with a good understanding of mission requirements or desired performance targets, the suite of available options and their performance under a wide range of disruptions scenarios, and the factors involved in determining the costs and risks associated with each.

The remainder of this chapter is divided into four sections. First, we describe the current arrangement and usage of electric power infrastructure, the risks that electric power and similar infrastructure face during military conflict, and how DoD has historically approached mission resilience to power disruptions. Second, we describe three broad categories of outside-the-fence options that may be available to DoD in different contexts. This section also discusses three key contextual factors that influence the ease of implementation of these outside-the-fence options. Third, we examine two distinct case studies, one for electric power and one for water—another critical infrastructure in which DoD has engaged in outside-the-fence activities to improve mission assurance through improved resilience. We conclude by considering key lessons as they pertain to electric power resilience and deterrence.

Electric Power Infrastructure

We begin by describing the current electric power system to clearly define which elements of the system are inside the fence versus outside the fence from DoD's perspective. Second, we provide examples of

---

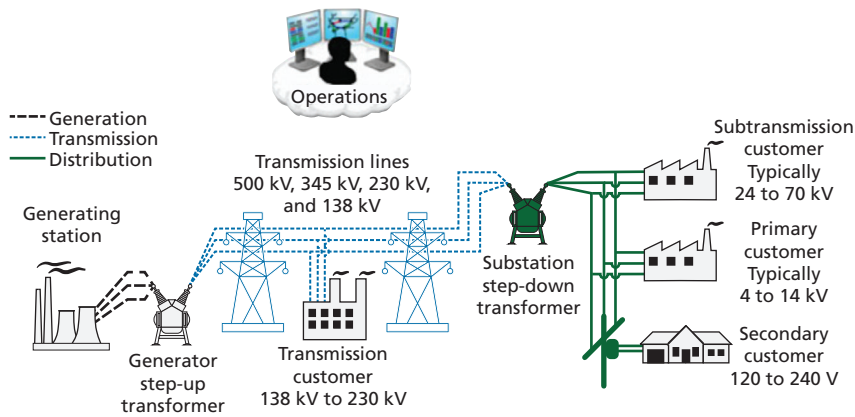
the U.S. power grid using cyber means (Perlroth and Sanger, 2018; Sanger, 2018). And the private sector is certainly not immune to cyber risk; a software failure was a key factor in the Northeast blackout of 2003 (Verton, 2003).

how this system can fail, including novel analysis of the documented risks faced by electric power and similar infrastructure during conflicts. Finally, we discuss how DoD has historically and recently sought to mitigate the risks associated with power system failure, both inside and outside the fence.

Current Electric Power Infrastructure

As shown in Figure 2.1, the U.S. electric grid consists of small and large facilities that produce power, high-voltage transmission lines for moving large amounts of power efficiently over great distances, lower-voltage distribution lines for distributing power to customers, and customers who consume power. The transmission lines of the U.S. grid interconnect power-generation and power-distribution facilities to create three distinct grid segments: the Western Interconnection, the Eastern Interconnection, and the Texas Interconnection. These systems are governed by a series of cyber and regulatory structures (such as control room operators who use operational technology to manipulate machinery to balance loads) and local, state, and federal regulatory agencies whose regulations determine reliability, security, and infrastructure maintenance regimes. Today, DoD's role is largely as a major

Figure 2.1
Current Electric Power System Structure



SOURCE: Based on figures from NIST, 2010, and Union of Concerned Scientists, 2015.

consumer of electricity rather than as a primary generator or distributor of electricity.[3] This means that many elements of the electric grid are largely outside the fence for DoD because they are owned, operated, and regulated by entities other than DoD.

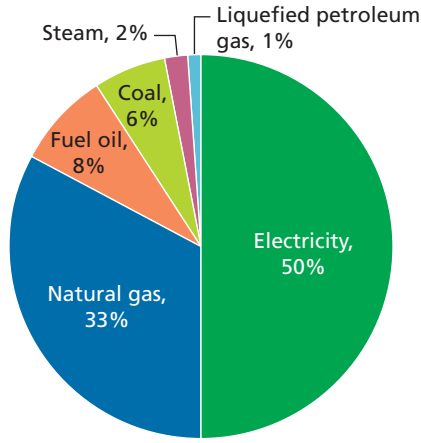
Many events, including natural hazards, equipment failures, operator errors, physical attacks, and cyberattacks, can disrupt the electric grid. Equipment failure, natural hazards, and operator error contribute to the majority of blackouts in the United States (Hines, Apt, and Talukdar, 2008). Blackouts, however, often have multiple causes; for example, weather, maintenance failure, and failure of a cyber system all contributed to the 2003 Northeast blackout, which left 55 million people across North America without power (U.S.-Canada Power System Outage Task Force, 2004). In addition, interdependencies between the power grid and other infrastructure, such as water and communications, can mean that failures in electric power systems lead to failures in other infrastructure and vice versa (Luiijf et al., 2008).

DoD's fixed installations are directly dependent on power for operations; in FY 2015, DoD spent $3.7 billion to power, heat, and cool buildings. As shown in Figure 2.2, half of DoD's installation energy consumption is in the form of electricity (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, 2016), and 99 percent of the electric power used by military installations comes from the civilian power grid (Andres and Breetz, 2011).

Power outages can affect DoD's ability to achieve its mission. Disruptions to power supplies, regardless of whether they are caused by determined adversaries, natural hazards, or other events, can disable or completely close military installations, necessitating the development and implementation of continuity of operations plans for critical missions (Marqusee, Schultz, and Robyn, 2017). DoD also relies on critical infrastructure that is dependent on electric power, such as water and communications, and access to such facilities would be lost if the power goes out. Furthermore, because military installations are often

[3] Some military installations are starting to generate some of their own power, including small projects using solar rooftops and hot-water heaters and larger projects using large-scale solar arrays and biofuel (often in partnership with industry experts).

Figure 2.2
DoD Installation Energy Consumption, by Source, FY 2015



SOURCE: Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, 2016.

located in outlying areas, they experience longer-duration and more-frequent outages than the typical utility customer (Marqusee, Schultz, and Robyn, 2017).

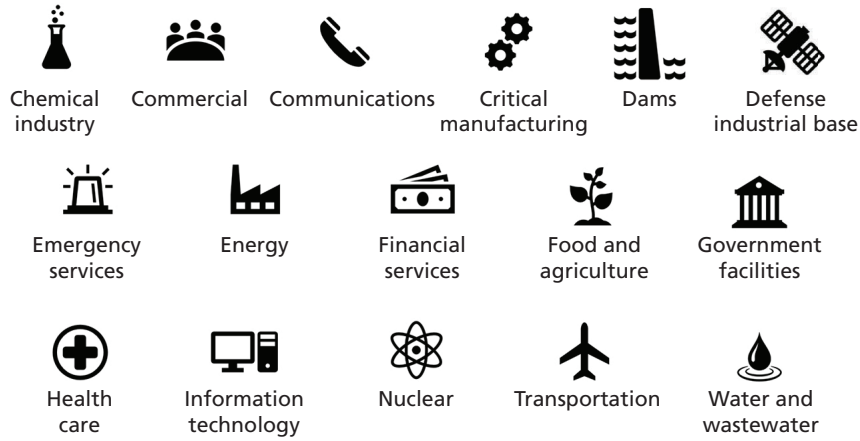
How Outside-the-Fence Infrastructure Has Been Treated During Armed Conflicts

Because blackouts can limit the ability of DoD or other entities to conduct military missions, it is conceivable that outside-the-fence electric power infrastructure would be an attractive target during military conflicts. However, the scale and scope of the risk faced by outside-the-fence electric power or other infrastructure during military conflict have not been thoroughly studied. In this section, we identify infrastructure that could be considered similar to the electric power system and discuss the treatment of both electric power and similar infrastructure during conflict scenarios. History shows that outside-the-fence infrastructure upon which civilians and the military rely has indeed been at risk during conflicts, highlighting the importance of potential efforts by DoD or others to engage in interventions to reduce this risk.

To identify infrastructure that is "similar" to the electric power system, we looked for infrastructures that share attributes with the electric grid. We began by examining existing lists of critical infrastructure. A National Consortium for the Study of Terrorism and Responses to Terrorism report (Miller, 2016) identifies 16 categories of critical infrastructure, including energy (see Figure 2.3). This list provides a useful initial categorization of infrastructure, although many types of infrastructure could be considered critical under different definitions of that word. To further narrow the selection, we looked for categories of infrastructure that share additional attributes with energy, and specifically with electric power.

Because our focus on electric power infrastructure is largely due to how critical it is to DoD's mission assurance, we searched for examples of outside-the-fence engagement in other infrastructures that play a key role in mission assurance for DoD. In a broadly interconnected world, the failure of any one of these systems could have severe implications for DoD's ability to accomplish its mission. In some cases, such as with electric power, water, and communications, the impacts might be relatively immediate, with severe failures effectively resulting in the temporary closure of military installations. In other cases, such as

Figure 2.3
Categories of Critical Infrastructure



SOURCE: Based on categories identified in Miller, 2016.

with critical manufacturing or financial services, the impacts of a failure would still be serious but might be less immediate. For our non–electric power case study, we opted to examine a type of infrastructure for which failure would result in relatively immediate impacts.

This report focuses on attacks by determined adversaries rather than on terrorist attacks. Some denial approaches that would deter a determined adversary could also deter terrorists or adversaries who are targeting civilians in pursuit of military advantage.[4] Indeed, broad-scale bombardments of cities and "scorched-earth" conquests have long been standard techniques in warfare. Attacks on infrastructure could also be highly targeted efforts, such as the Stuxnet program that targeted Iranian nuclear centrifuges (Zetter, 2014). Or such attacks might be inflicted by retreating armies that would destroy infrastructure rather than let opponents capture and use it. Historic examples include retreating Iraqi forces setting fire to Kuwaiti oil wells during the Persian Gulf War, German forces destroying most road and rail bridges across the Rhine as they retreated from Allied forces in World War II, and the nomadic Scythians burning the land and poisoning water supplies as they retreated to avoid engaging with the advancing Persian army of King Darius in 513 BCE, which contributed to Darius eventually abandoning the Persian advance.[5]

---

[4] Adversaries might or might not actively avoid civilian disruption in pursuit of military advantage. Disruption of civilian use of infrastructure might be pursued in a campaign aimed to decrease civilians' support for their nation's military involvement in a conflict (Schaffer, 1980). The strategic bombing campaigns of World War II explicitly targeted key nonmilitary infrastructure with the goal of crippling adversaries by disrupting their economies. Alternatively, an adversary might avoid disruption of civilian use of infrastructure during a "hearts and minds"–style campaign, in which leaders of a military engagement desire to maintain some level of support from the local population (Berman, Shapiro, and Felter, 2011).

[5] Indeed, one perception of warfare is that it is an effort to defend or capture infrastructure and other resources. Herodotus, speaking from the perspective of the nomadic Scythian king on his avoidance of the Persian offensive, wrote, "We have no cities—nothing that we need worry you might capture. We have no crops—nothing that we need worry you might destroy. Why, then, should we be in any rush to fight with you?" (Holland and Shore, 2017; Hays, 2016).

The question of what types of infrastructure are at higher risk during military conflicts is objective and measurable, although, to our knowledge, such analysis has not been published; related publications and data sources focus on infrastructure at risk from terrorism.[6] There is no single existing database designed to support an analysis of infrastructure risks during armed conflict. To provide an initial examination of this issue, we reviewed a wide variety of relevant databases to determine which contained information on military attacks on infrastructure. We ultimately present information from four data sources: the Air Force Research Institute (AFRI) Theater History of Operations (THOR) database, the International Institute for Strategic Studies (IISS) Armed Conflict Database (ACD), the Center for Strategic and International Studies (CSIS) Significant Cyber Incidents list, and the Council on Foreign Relations (CFR) Cyber Operations Tracker.[7]

The THOR database contains more than 900,000 records of the dates and targets of airstrikes by U.S. and Allied forces during World War I, World War II, and the Vietnam War. An advantage of using this data set is that it provides a structured record of military attacks on infrastructure. Downsides of using this data set are that it does not include recent attacks on infrastructure or attacks by U.S. adversaries. To address these downsides, we examined information from the ACD, which does include recent attacks by U.S. adversaries. The ACD provides text descriptions of a large variety of recent attacks. However, many recorded attacks do not involve infrastructure, and extracting data relevant to this exercise had to be done manually. Due to time limitations, we collected data only on attacks on infrastructure during the recent and ongoing conflict in Ukraine. Finally, because both the THOR database and the ACD generally focus on kinetic

[6] Examples of major published databases that assess infrastructure risk from a terrorism perspective include the National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database, the Energy Builders Energy Infrastructure Incident Reporting Center, the Jane's Terrorism and Insurgency Centre, the International Institute for Counter-Terrorism's Incidents and Activists Database, the U.S. government–funded American Terrorism Study, and the RAND Database of Worldwide Terrorism Incidents.

[7] To access these publicly available data sources, see AFRI, undated; IISS, undated; CSIS, undated; CFR, undated.

attacks, we also examined data on cyberattacks from the CSIS and CFR sources, which each include examples of state-sponsored cyberattacks on infrastructure.

Along with the historical examples discussed earlier, these data emphasize that attacking nonmilitary infrastructure to gain military advantage has been a common practice both historically and more recently. Table 2.1 shows that attacks on transportation infrastructure are particularly common, although these cases might include attacks on military resources located at those locations, or the locations themselves might be military-owned facilities or transportation vessels. We also see many attacks on facilities that support military activities but are likely not owned by the military, such as factories, electric power grids, and chemical plants. The focus of this table is not on the specific numbers of attacks. Rather, its purpose is to provide clear evidence that civilian infrastructure that directly or indirectly supports military missions has been a target during past conflicts.

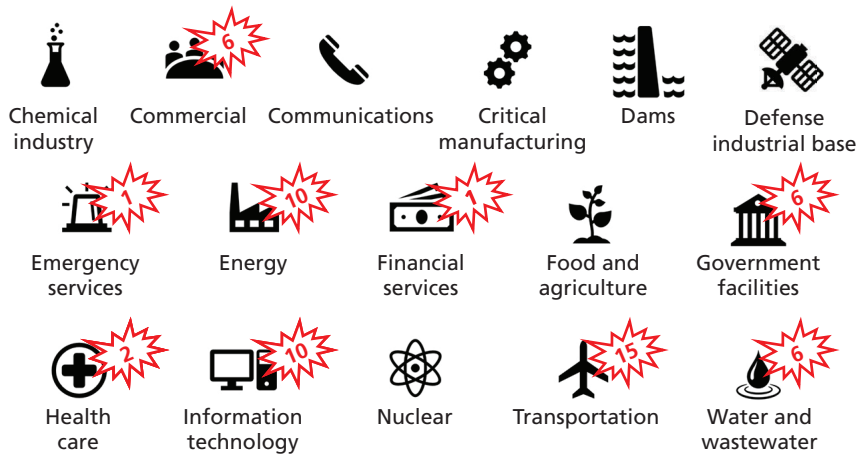
Figure 2.4 shows that similar patterns are exhibited in attacks involving U.S. adversaries. Attacks that the ACD recorded as being implemented by "pro-Russian separatists" or "unknown" actors against

Table 2.1
Attacks on Infrastructure by U.S. and Allied Forces During World War I, World War II, and the Vietnam War, by Targeted Infrastructure

Targeted Infrastructure	Number of Attacks
Roads	58,673
Bridges	44,000
Railroads	18,933
Shipping facilities	6,934
Fuel depots	3,585
Factories	2,082
Electric power	530
Chemical plants	239

SOURCE: RAND analysis of the THOR database (AFRI, undated).

Figure 2.4
Number of Attacks on Ukrainian Infrastructure, by Category, 2014–April 2018



SOURCE: RAND analysis of ACD records of attacks by "pro-Russian separatists" or "unknown" actors against Ukrainian infrastructure (IISS, undated). The categories of infrastructure were identified in Miller, 2016.

Ukrainian infrastructure include many attacks on transportation and energy infrastructure, as well as on water and wastewater systems, government facilities, and commercial facilities.

In addition to being targeted by kinetic attacks, critical infrastructure systems have become targets of cyberattacks. The CSIS Significant Cyber Incidents list recorded 20 state-sponsored cyberattacks between July 2016 and July 2017 that targeted critical infrastructure. Fourteen were for the purpose of espionage, but the remainder reflect new, emerging types of cyberattacks that aim to destroy data, steal money, or sabotage systems. In 2015, the first electric power outage caused by a cyberattack occurred in Ukraine, causing an outage for more than 230,000 residents that lasted up to six hours in some areas (Greenberg, 2017a; CFR, undated). The attackers also flooded customer service phone lines, preventing customers from reporting the outages (CFR, undated). A second power outage caused by a cyberattack occurred in Ukraine in 2016. These attacks highlight that criti-

cal infrastructure systems, especially power grids, can be targeted by cyber means.

How DoD Has Approached Mission Resilience to Power Disruptions

Currently, DoD engages in a variety of inside-the-fence resilience efforts. These include backup power-generation sources, such as fixed and mobile generators, combined with uninterruptible power-supply systems. One challenge with this approach is that reliance on fuel-based generators makes long outages that disrupt fuel delivery services particularly problematic (Narayanan et al., 2017). There has also been significant interest in microgrids and a wide variety of types of on-installation electric power production. Individual missions also have continuity of operations plans, which identify backup plans and alternative mission locations in the event of a power outage.

DoD can and has used multiple approaches to both increase the resilience of the power grid and reduce the cost of electricity. These approaches include utility privatization, intergovernmental support agreements (IGSAs), energy-saving performance contracts, public-private partnerships, and energy outgrants.[8] Authorizations and guidance to pursue these various partnership-based approaches to increasing resilience typically come from Congress and DoD. For example, congressional legislation in 1997 provided legislative authority for utility privatization on military installations, and, in 1997, DoD issued Defense Reform Initiative Directive #9, which directed military departments "to develop a plan for privatizing all of their utility systems (electric, water, waste water and natural gas) by January 1, 2000, except those needed for unique security reasons or when privatization is uneconomical" (Hamre, 1997). Under this authority and other partnership authorities, military installations continue to experiment with a variety of public-public partnerships and public-private partnerships that hand off responsibility for operations and management of on-

[8] Utility privatization is an approach in which DoD engages in long-term contracts to provide a temporary conveyance of DoD infrastructure to a non-DoD entity that manages the systems. Under this setup, the non-DoD entity is incentivized to invest in maintenance and system efficiency and resilience updates on DoD's behalf.

installation electricity distribution systems to non-DoD entities, with the goals of reducing long-run life-cycle costs, using renewable energy sources, and improving the reliability of military installations' access to the primary generation grid (Lachman et al., 2011; Lachman, Resetar, and Camm, 2016; Lachman et al., 2016).

DoD has also pursued a variety of outside-the-fence approaches to support reliable access to electric power. For example, DoD has leased land to allow private power-generation facilities to be built on installation property, in exchange for DoD having first-access rights to purchase power produced by that facility. In the event of a power outage, this could ensure that the installation can resume operations quickly.[9] In at least one case, an Air Force installation has shared the cost of building and operating a nearby high-voltage electrical transmission line with a local utility provider (Lachman et al., 2016). Additional examples of such partnerships are provided later in this chapter in the section on our first case study.

In addition to its efforts aimed at gaining access to multiple power sources, DoD has focused on reducing overall electric power consumption, largely in an attempt to lower spending on electricity (Lachman et al., 2011). Such efforts to reduce electricity costs often have secondary benefits for resilience. For example, lower overall consumption means that less backup capacity is required, and replacing inefficient system components with new, more-efficient parts can improve reliability if the new parts are less likely to fail.

Our review of DoD's past and ongoing strategies for investing in power resilience points to a need for a structured framework, particularly when it comes to making decisions about when and how to pursue outside-the-fence interventions.[10]

---

[9] Not every instance of private power generation on a base leads to direct benefits for the base. In some cases, the electricity might be routed to the grid, and the base sees no improvements in power resilience.

[10] Military departments already have rules and regulations describing when, where, and how to pursue inside-the-fence interventions, such as when backup generation is required and how it is to be maintained. For example, see Department of the Air Force, 2015.

Intervention Framework

This section describes broad categories of outside-the-fence interventions that might be available to DoD in different settings and identifies factors that could influence the ease of implementation of these options. We refer to the articulation of the three categories of outside-the-fence options and the three contextual factors that influence the implementation ease of these options in different settings as a *framework* because it is intended to provide a conceptual structure upon which future discussions and analysis can build. We draw on literature reviews and two case studies (detailed later in this chapter) to develop categories of outside-the-fence interventions, and we identify contextual factors that are likely to influence the implementation ease of each category of intervention. All identified interventions are captured by these categories, but the categories are not necessarily assumed to be exhaustive.

Types of Outside-the-Fence Engagement

We use three broad categories to describe outside-the-fence interventions that DoD can use to support electric power resilience: shifting the fence line, influencing governance, and leveraging resources. Figure 2.5 depicts the path for how DoD could use outside-the-fence interventions to improve mission assurance. Specific *interventions* are pursued for the purpose of achieving one or more *outputs*, such as obtaining new or more-efficient infrastructure, establishing backup systems or other redundancies, or establishing or altering processes or contingency plans. These outputs are pursued because they directly or indirectly result in *outcomes*, such as improved electric power reliability. These outcomes directly affect *mission assurance*, and improving mission assurance is DoD's ultimate objective.

Figure 2.5
Path for Using Interventions to Influence Mission Assurance

The first category of outside-the-fence interventions, *shifting the fence line*, includes any actions that change whether a specific aspect of the power grid (or other critical infrastructure system) is owned or operated by DoD or a non-DoD entity. One approach to such an intervention is to use utility privatization agreements. These agreements are increasingly common for such utilities as electricity, gas, water, and wastewater. According to the U.S. Government Accountability Office (2018, p. 1), DoD "has privatized nearly 600 of about 2,600 utility systems on military installations worldwide, including electric, water, wastewater, natural gas, and thermal systems." In addition, it has issued broad guidance for determining whether to pursue utility privatization (DoD, undated).

Shifting the fence line also includes efforts that place non-DoD elements of the power grid (or other critical infrastructure) under DoD control. For example, during World War I, the federal government briefly took control of both the railroad system and the telephone system (Janson and Yoo, 2013). But shifting the fence line can include more-nuanced measures than simply taking full ownership. During World War II, the U.S. Army provided security to the Bonneville Dam area, stationing almost 200 soldiers there and mounting a .50-caliber machine gun inside the powerhouse (Figure 2.6). It did so because the dam provided electric power to the shipyards in Portland, Oregon (and to Hanford Engineer Works, which was secretly producing plutonium for atomic bombs), making the dam a possible target for enemy attack (Willingham, 1992).

The second category of outside-the-fence interventions, *influencing governance*, includes efforts to directly or indirectly influence how the electric power infrastructure system works, such as through directly or indirectly changing rules, regulations, or processes. For example, DoD might participate in contingency planning exercises, as it did with the President's Commission on Critical Infrastructure Protection (1997). DoD might also lobby non-DoD entities to encourage certain regulatory changes, or it might negotiate with local service providers to arrange priority treatment for DoD facilities during a power outage. Note that simply influencing governance would not automatically mitigate risk. DoD would need to additionally work with power

Figure 2.6
Pillbox Outside Bonneville Dam Constructed During World War II

SOURCE: Photo by Aaron Clark-Ginsberg.

regulators to ensure that utilities are granted the required permits and offered the right incentives (e.g., a higher rate of return on capital) to make the necessary system upgrades.

The third category, *leveraging resources*, includes efforts to use money or other resources, such as land or people, to arrange or influence outside-the-fence outcomes. Examples of this method are contractual arrangements with local utilities or local governments to share the cost of a common resource (e.g., a shared power line or water main) and contractual arrangements in which DoD provides on-installation land to a private energy company for the construction of a power-generation facility in exchange for first-access rights to the power produced by the constructed facility.

DoD engages in these activities with the goal of achieving certain outputs, such as obtaining new or more-efficient infrastructure, establishing backup systems or other redundancies, or establishing or altering processes or contingency plans. Any particular outside-the-fence intervention could achieve one or more of these outputs. However, the ease with which these outside-the-fence options can be implemented can vary significantly. In the next section, we discuss contextual factors that might influence that ease of implementation.

Determining When and How to Engage

The choice of which type of outside-the-fence intervention to use would be greatly simplified if there were a clear, quantitative model for assessing and predicting the relative benefits and costs of each intervention across a range of different scenarios. Unfortunately, such a model does not currently exist. The goal of this section, and the rest of this chapter, is not to create such a model but rather to identify key elements that it might entail.

The complexity of infrastructure systems makes it difficult to fully understand and quantitatively model the costs and benefits associated with outside-the-fence methods of intervention. This is because any given infrastructure system involves a complex mix of interacting people, processes, and technologies. In other words, such systems "consist not only of hardware, but also of legal, corporate, and political-economic elements. . . . [I]nfrastructures are not merely large systems, but sociotechnical *institutions*" (P. Edwards, 2003, pp. 199–200). They are owned and operated by a mixture of stakeholders; regulated by various agencies—both governmental and nongovernmental—at local, national, and international levels; and contain a multitude of diverse and complex technologies. For instance, the electric power system spans the continental United States; is interconnected with the power grids of Canada and Mexico; and comprises dozens of governmental bodies, more than 3,000 small and large public and private utilities, 5,800 major power plants, 450,000 miles of high-voltage transmission lines, and numerous standards and regulations (American Public Power Association, 2015; Executive Office of the President, 2013). And in the

past, changing regulations and associated technologies have increased complexity (Hirsh, 1999; Latham, 2003; Perrow, 2007).

Despite this complexity, there are many examples of studies that consider the costs and benefits associated with implementing new outside-the-fence solutions or scaling up existing solutions. Often these studies focus on assessing the mechanical impacts of implementing a new technology or expanding the use of existing technology. Indeed, there is useful guidance on how to conduct proper cost-benefit analyses.[11] Although they are critical inputs to investment decision-making, these types of analyses are not sufficient on their own. Other, less-explored factors can influence the ease with which different interventions can be implemented. Drawing on case studies and a literature review, we identify three contextual factors that might influence the availability and feasibility of various outside-the-fence interventions: ownership, relationships, and laws and regulations.

Ownership

Ownership refers to the stakeholder(s) who, through property rights or other titles, have legal responsibility and the associated decision-making authority over a given infrastructure component or resource. When DoD owns an infrastructure component, shifting that ownership outside the fence line becomes an option, although, in some cases, this has required congressional approval.[12] As discussed earlier, DoD has sometimes taken control of non–DoD-owned infrastructure, although such interventions can be controversial and may be feasible or prudent only under extreme circumstances. For cases in which DoD does not own the infrastructure, interventions that influence governance or leverage resources might be less controversial. Interventions that leverage resources require DoD to offer a non-DoD entity the

[11] DoD staff seeking to implement outside-the-fence investments can consult the *Department of Defense Guidance for Privatizing Defense Utility Systems* (DoD, undated), DoD's *Economic Analysis for Decision-Making* (DoD, 2017), and the "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs" (Office of Management and Budget, 1992).

[12] For example, in the National Defense Authorization Act for Fiscal Year 1998 (Pub. L. 105-85, 1997), Congress approved legislative authority for privatizing utility systems at military installations.

right to use a related resource that is DoD-owned. For example, DoD is able to offer the use of on-installation land for the construction of power-generation facilities because DoD owns that land. In contrast, the Bureau of Land Management is the lead agency for mineral rights on federal land, including military installations,[13] so DoD must coordinate any mineral-related easements with the bureau and might not have access to any resulting revenue.

Relationships

One finding from the case studies discussed later in this chapter is that outside-the-fence interventions seem to appear where DoD has developed long-standing relationships with the related non-DoD entities. We cannot say definitively whether building more or stronger relationships with these entities would improve DoD's ability to engage in outside-the-fence interventions. On the one hand, building such relationships could reduce the costs of outside-the-fence interventions by reducing transaction costs, improving communications, and increasing reliability. On the other hand, focusing solely on working with organizations with which DoD has established long-standing relationships might limit DoD's options for outside-the-fence interventions. Regardless, building or maintaining long-standing relationships appears to play a role in the cost of pursuing, developing, and implementing outside-the-fence interventions.

Laws and Regulations

Regulations are a core component of infrastructure systems, shaping how they are designed and used. Although infrastructure owners have significant influence over what is done and how it is done, the types of activities that owners can and cannot pursue are restricted by laws and regulations. Specific to our purposes, laws and regulations can restrict the types of outside-the-fence interventions that federal agencies, including DoD, can engage in and how the contractual agreements must be structured. Such laws and regulations include the Federal Acquisition Regulation (FAR), Office of Management and Budget

[13] For information on the Army coordinating with the Bureau of Land Management on mineral exploration and extraction, see Department of the Army, 1984.

Circular A-11 and Circular A-76, small and disadvantaged business set-asides, and AbilityOne contracts (Lachman et al., 2016).

Laws and regulations offer an opportunity for DoD to engage in the type of outside-the-fence interventions that we categorize as influencing governance. The FAR offers one example of how DoD can improve mission assurance by engaging with the regulatory process. In particular, the FAR sets requirements for federal government procurement of goods and services. Initially, military installations needed to follow FAR procedures in developing IGSAs "when the total purchases (i.e., acquisitions) by the federal government using appropriated funds are at or above $150,000 in one year or $30,000 per year over five years" (Lachman, Resetar, and Camm, p. xviii). DoD initially interpreted the FY 2013 NDAA as requiring "the use of the FAR for all IGSAs involving the provision of goods and services to the government" (Office of the Assistant Chief of Staff for Installation Management, undated). This created problems for DoD: "Because municipalities have no or limited experience with the FAR, they were cautious about entering into contracts without detailed understanding of each clause. This slowed progress on IGSAs" (Office of the Assistant Chief of Staff for Installation Management, undated). The FY 2015 NDAA ultimately clarified that the FAR is not required for IGSAs; each service secretary can now determine the appropriate legal instrument for his or her setting. Communicating DoD needs can be key to obtaining such changes. In October 2014, DoD issued appeals on several aspects of the FY 2015 NDAA, including on language about potential requirements involving the procurement of services (Office of the Assistant Secretary of Defense for Legislative Affairs, 2014).

Although many regulations and laws are focused on encouraging transparency, safety, and efficiency in infrastructure, pursuit of these goals could indirectly result in improved reliability of infrastructure systems. Other regulations may incorporate reliability or resilience directly, such as by requiring infrastructure owners and operators to follow specific risk management requirements. For example, the North American Electric Reliability Corporation's critical infrastructure protection standards and its reliability standards impose cybersecurity

and reliability requirements, respectively (see North American Electric Reliability Corporation, undated).

Engaging with regulatory processes requires identifying the appropriate regulatory agency to work with. A sector may face federal, state, or local government-imposed regulations, as well as self-imposed industry standards. Although many industries do self-regulate, there is little reason for industry to defer to DoD requests without some financial or regulatory incentive to support the associated investment. And although national security can be framed as a matter of corporate social responsibility (Ridley, 2011), there is limited evidence that infrastructure owners and operators will implement risk management activities that are detrimental to their bottom line in a market-driven space (Quigley, 2013).

Case Studies

Supplementing our review of the literature, we used two case studies to help understand how ownership, relationships, and laws and regulations might affect the implementation ease of outside-the-fence intervention options. The first case study focuses on electric power in the context of a resilience-boosting option that DoD is currently pursuing. The second case study focuses on water infrastructure and considers an option that DoD *could pursue* but has not yet.

Case Study 1: Electric Power at Tinker Air Force Base

Tinker Air Force Base (AFB), in Oklahoma City, Oklahoma, offers an example of DoD's efforts to engage in outside-the-fence activities in the electricity sector. Tinker AFB has engaged in outside-the-fence partnerships with Oklahoma Gas and Electric (OG&E) to improve the resilience of its electric power supply since at least 1974 (Saxton, 2017). OG&E provides electric power to customers in Oklahoma and Arkansas, and its prices and service reliability are regulated by the Oklahoma Corporation Commission. The commission can have considerable influence over OG&E's prices and, hence, its ability to pursue

any upgrading and expansion activities (U.S. Securities and Exchange Commission, 2005).

Various Partnerships

Tinker AFB has had several different types of partnerships to help improve energy resiliency. First, in 1988, Tinker AFB and OG&E partnered to install an 80-MW peaking generating station at the base. Tinker AFB provided a long-term ground lease to OG&E at no cost (Federal Utility Partnership Working Group, 2008). In return for the land lease, Tinker AFB has top priority in purchasing electric power from the plant, and the station allows Tinker AFB to separate itself from the rest of the power grid if needed. OG&E owns, operates, and maintains the station; Tinker AFB provided the land and pays for the cost of any electricity it purchases. This partnership deal has been important for long-term installation energy resiliency.

Second, in 2010, OG&E and Tinker AFB signed an electric utility privatization contract that allowed OG&E to take over the electric distribution system at the base. Under the 50-year contract, awarded in September 2010, "OG&E will assume ownership of the electric system at Tinker. The company also will be responsible for its operation and maintenance" (Marks, 2010). However, there was a two-year process before OG&E personnel were able to have an increased presence on the base. According to a Tinker AFB news announcement,

> Before the contract could be enacted, the Oklahoma Corporation Commission, which regulates OG&E, had to review and agree to the terms. Following the approval in September 2011, OG&E personnel began familiarizing themselves with Tinker's inventory and systems, and mapped locations of equipment including transformers, manholes and lines. (O'Brien, 2012).

This privatization of the base electric distribution system is part of a larger trend of increasing partnerships to help manage and operate installation facilities and infrastructure.

Third, in 2016, a $19.1 million facility renovation project focused on upgrading the central utility plant that serves Tinker AFB's 2.6 million ft^2 assembly plant. Under this project, led by OG&E, Honeywell

installed new, more-efficient systems, which are intended to resolve mechanical problems ranging from leaks to temporary boilers that required round-the-clock management; in addition, the changes are expected to reduce annual energy consumption at the plant by 44.3 percent (Parker, 2016), saving $3.5 million per year (Casey, 2016). Military installations often have neither (1) the funds available to pay large lump sums for the major maintenance updates that can both improve reliability and reduce costs nor (2) the authority to take on additional debt. Instead, the project is funded through a utility energy service contract, which means that the $19.1 million is paid as Tinker AFB continues to pay its preexisting utility rates, and contractors are funded through the savings produced. A Honeywell press release notes, "The contract enables the base to pay for the project using future energy savings generated by the more efficient energy, water and renewable systems to be installed. Honeywell is providing the upgrades and guaranteeing the savings" (Honeywell, 2016).

Fourth, in a separate partnership between Tinker AFB and Honeywell that uses an energy savings performance contract, Honeywell was subsequently awarded a $262 million project in 2017 to modernize an additional 10 million ft^2 of space across 50 buildings at Tinker AFB. This award is the largest energy savings performance contract the Air Force has awarded to date (Dupree, 2017).

These partnerships provide clear examples of several intervention methods described in the framework discussed earlier in this chapter. The 1988 construction of a generating station is an example of DoD leveraging resources to improve the resilience of its electric power supply. Rather than pay to construct and maintain its own generation facility, Tinker AFB was able to leverage two resources—land and a steady stream of future utility payments—to make OG&E benefit from building and maintaining an on-base station. The 2010 privatization of the base distribution system provides an example of DoD shifting the fence line to increase electric power resilience. Maintenance responsibilities were also shifted from Tinker AFB to the private sector. The 2016 modernization effort reflects both leveraging resources and shifting the fence line. Although obtaining large lump sum amounts to hire contractors is often infeasible, Tinker AFB was able to leverage

its preexisting stream of utility payments to finance the modernization of its facilities by private-sector entities, with the private sector bearing much of the financial risk.

Takeaways

There are two main lessons to learn from this case study. The first is that the large, successful outside-the-fence interventions seem to have been built with entities that had long-term relationships with DoD. In many cases, a successful small project led to increasingly ambitious projects with the same partners. Furthermore, complicated deals take time to develop: OG&E had been working to secure the 2010 privatization arrangement since 2004 (Marks, 2010).

The second lesson is that outside-the-fence arrangements can provide benefits not available through traditional inside-the-fence methods. As of 2008, Tinker AFB had approximately 72 backup generators (Weston Solutions, 2008). However, the outside-the-fence efforts discussed in this section promote electric power resilience at Tinker in a way that simply building additional backup generators cannot. The 1988 partnership that leased land for the construction of an 80-MW peaking generation station ensured that Tinker AFB would have easy access to a reliable electric power source. Leaders at Tinker AFB viewed the privatization of its electric distribution system as beneficial, in part, because that approach would improve the resilience of the base electricity supply. In a news announcement from Tinker AFB, electrical engineer David Holt explained, "OG&E has lots of staff and equipment, more so than the government. If we were to have an ice storm or tornado, they can respond and get that fixed a lot quicker than we would be able to; we don't have the resources they have" (O'Brien, 2012).

The environmental benefits of these arrangements are laudable, but deals this large are not made purely to address environmental concerns. These partnerships are about improving mission assurance through improved resilience, and, in some cases, the partnerships reduce costs at the same time. It is also important to note that, although these particular efforts have worked well for Tinker AFB, the optimal interventions for improving mission resilience through electric power resilience are likely to vary from installation to installation.

Case Study 2: Water

DoD relies on water and wastewater in its military installations as a source of drinking water and to cool its computers and electronic systems; provide for fire suppression; and operate other critical infrastructure, such as hospitals, whose patients and medical providers need a steady supply of water (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, 2016). In FY 2016, DoD facilities consumed 85.5 billion gallons of potable water (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, 2017). Like electricity, water and wastewater services are necessary for DoD to execute its missions.

Water Systems and DoD Mission Assurance

DoD's water supply and quality can be compromised in many different ways, including physical, cyber, and biological attacks; maintenance failures; natural hazards, such as earthquakes, hurricanes, and wildfires; and breakdowns in other infrastructure that the water system depends on, such as electricity. Compromising an installation's water supply or quality can cause direct impacts, forcing the closure of key facilities or leading to health problems that are realized years or decades later. Indirect impacts can also be created when other infrastructure is compromised due to the political and economic impacts associated with water disruption. Although it is unknown how frequently installations have to close for water-related reasons, drinking-water contamination is a problem for many military installations, as indicated by 2018 testing that found contaminants linked to cancer and birth defects at 126 installations (Copp, 2018). Given their dependence on water for cooling electronic systems, fire suppression, and other drinking and nondrinking needs, DoD military installations could be seriously affected if water and wastewater services were to become unavailable (Stockton, 2016).

The military's dependence on water systems could make such systems a tempting target for a determined adversary during a military confrontation. This risk is further emphasized by recorded attacks on water and wastewater infrastructure during conflicts involving U.S. adversaries. For example, during the ongoing conflict between Russia

and Ukraine, shelling targeted the Donetsk Water Filtration Station on three consecutive evenings in November 2017, and additional nearby explosions were recorded several days later. During the same period, the Verkhniokalmiuska Water Filtration Station was hit more than 12 times in a single night (IISS, undated; Walker, 2017). In addition to the risk of disrupting the local water supply, both stations store large chlorine gas containers that could release fatal quantities of chlorine gas if punctured. Earlier in the same conflict, exchanges of fire in Avdiivka left the city without electricity or water services in July 2016 (IISS, undated).

DoD guides its approach to water management through policies and strategies, including the *Joint Bulk Petroleum and Water Doctrine* (Joint Chiefs of Staff, 2016); the *Army Water Security Strategy* (Marstel-Day, 2011), which describes the Army's strategy for improving water security; and *Emergency Response Planning for Military Water Systems* (U.S. Army Center for Health Promotion and Preventive Medicine, 2005). DoD's use of water is also beholden to 1997 Defense Reform Initiative Directive #9, which calls for privatizing utility systems (Hamre, 1997).

DoD is reliant on governmental, nongovernmental, and private infrastructure providers for its water. These providers consist of 151,000 public water systems, which are mainly small and municipal-owned systems, but a few are larger privately owned systems (U.S. Environmental Protection Agency, undated). Although many are small, the largest, American Water, had a $3.3 billion operating revenue in 2016 and employed 6,800 employees across 47 U.S. states and Canada. These water providers are guided by several different regulatory and governance structures. All water systems serving a population of more than 3,300 must conduct a vulnerability assessment and develop an emergency response plan under the 2002 Public Health Security and Bioterrorism Preparedness and Response Act (Pub. L. 107-188). The water sector also has a Water Information Sharing and Analysis Center (WaterISAC), established in 2002 by an act of Congress. Presidential Policy Directive 21 (White House, 2013) designates the water and wastewater sector to be critical infrastructure and the Environmental Protection Agency as the sector-specific

agency. Certain regulatory regimes vary depending on their size and ownership. Smaller municipal-owned utilities are mainly bound under the American Water Works Association (AWWA)'s voluntary federal-level reliability and security standards, while larger utilities that are not municipal-owned also follow the regulations of state public utility commissions.

The *Army Water Security Strategy* notes that

> outside the fence line, significant water security issues may exist or arise that can directly affect the ability of the installation to perform its mission. Consequently, a more robust approach to water security requires situational awareness and effective action beyond the perimeter. (Marstel-Day, 2011, p. 14)

Since Defense Reform Initiative Directive #9, DoD has been transitioning ownership and operation of water infrastructure to utilities. For instance, DoD has established 50-year utility privatization contracts with American Water to own, operate, and maintain water services on 11 military installations (American Water, undated), and many other utilities provide similar services. For these installations, DoD provides physical security for water infrastructure, while the private contractors are responsible for the security of cyber assets. Another approach to increasing water security is forming partnerships with other entities, such as the collaboration between Fort Leonard Wood and Sustainable Ozarks Partnership, funded by the state of Missouri and the city of St. Robert, to interconnect the water systems of St. Robert and Fort Leonard Wood, providing reciprocating backup water services (Sustainable Ozarks Partnership, 2017).

DoD also sits on the Government Coordinating Council of the WaterISAC, which helps facilitate information-sharing. The Army Corps of Engineers is responsible for maintaining commercial waterways and operating dams and locks, which are the basis for many drinking water systems. Additionally, DoD could work with state and federal regulators to advocate mandatory reliability and security regulations, which would help standardize levels of risk mitigation. To reduce chances of water failure caused by the compromise of other

infrastructure, DoD could support federal efforts to identify cross-sector interdependencies, advocate that the Federal Emergency Management Agency prioritize restoring the water supply in response and recovery planning, or provide fuel for water utilities to use to power their backup generators in the event of an outage.

Fort Bragg and Water

Fort Bragg offers an example of DoD's approach to outside-the-fence water resilience. Located in Fayetteville, North Carolina, Fort Bragg is a large military installation with more than 50,000 active-duty personnel. Before 2010, Fort Bragg owned and operated its own water plant to provide the approximately 4 million gallons of water the base needed per day. In 2010, DoD transitioned ownership and operation of water infrastructure to private utilities, establishing contracts with three water providers: Harnett Regional Water, Fayetteville Public Works Commission (PWC), and Old North State Water Company. Harnett Regional Water and Fayetteville PWC together deliver water to the installation, alternating service provision days and delivering water through a 36-inch main pipe or a smaller secondary feed if the main pipe breaks. Inside the installation, water systems are managed by Old North State Water Company, which is responsible for all aspects of system maintenance and operations.[14]

This partnership model is useful for several reasons. The water utilities operate at an economy of scale that allows them to maintain high levels of specialized technical staff and equipment specific to water operations, so they can efficiently deliver high-quality and reliable service. The water utilities use the AWWA's standards as a performance benchmark. Reliability is further enhanced by mutual response agreements, including localized response agreements between the Fayetteville PWC and Harnett Regional Water, as well as state-level response agreements in place through N.C. Water WARN, a network of water utilities that assist each other during emergencies (North Carolina Environmental Quality, 2018). These utilities have indeed been

[14] The information in this paragraph is based on Fayetteville PWC staff, interview with the authors, July 24, 2018.

able to provide Fort Bragg with a source of water during emergencies. For example, in 2016, Hurricane Matthew compromised Fort Bragg's water supplies, but the Fayetteville PWC and Harnett Regional Water were able to provide the installation with a temporary source of water. Furthermore, because of Fort Bragg's high levels of water consumption and national security importance, the utilities consider it a key account and attempt to fix any disruptions rapidly.

Although the utilities are following AWWA's voluntary regulatory guidelines, there are no mandatory federal guidelines, and the voluntary guidelines do not have the same amount of specificity as mandated federal guidelines do when it comes to risk management interventions. As county governmental agencies, the Fayetteville PWC and Harnett Regional Water are also exempt from any state-level public utility commission rulings. These regulatory dimensions structure where DoD might intervene to affect water infrastructure resilience: Because local utilities are not guided by mandatory reliability or security regulations, DoD needs to work directly with local utilities rather than regulatory authorities in order to reduce risk. If DoD were to attempt to influence governance structures, it would have to interact with state and federal authorities, possibly to advocate making reliability and security regulations mandatory. Such interventions would then affect whom DoD might work with to reduce risk.

Takeaways

One takeaway from this case study is that shifting the fence line could enhance the reliability of water supply and delivery, which, in turn, could affect mission assurance. However, shifting the responsibility for water to utilities outside of DoD has not been a panacea: Fayetteville PWC has faced recent concerns about drinking-water quality.[15] This case study also illustrates that external operators and providers of water infrastructure, while generally able to maintain water systems and respond to water system failures when they arise, are not guided by strong regulations and are often reliant on other infrastructures that

[15] Tests of water from Fayetteville PWC found levels of 1,4 dioxane, a potential carcinogen, that are well above federal advisory levels (Barnes, 2018).

could fail. Other methods, such as influencing governance and leveraging resources, could be employed to reduce risks not addressed by shifting the fence line.

Lessons for Electric Power Resilience

DoD engages in a variety of both inside-the-fence and outside-the-fence efforts to ensure the resilience of its electric power supply. However, DoD needs a method for determining the ease of implementation of outside-the-fence interventions. We find that ownership, relationships, and laws and regulations play key roles in affecting the implementation ease of outside-the-fence interventions. A deeper characterization of these roles and the interactions among them can provide DoD with a structured approach to prioritizing investments in outside-the-fence resilience interventions.

We have also shown in this chapter that the risks to power grids are not hypothetical. Critical infrastructure not owned by the military, including electric power infrastructure, has often been a target during conflicts in both kinetic attacks and cyberattacks, and U.S. systems face real risks. Deterrence via resilience enhancements is one mechanism through which DoD might be able to reduce the likelihood of such attacks.

CHAPTER THREE

Punitive Options for Deterring Cyberattacks on the Power Grid

Following revelations of the current cyber threat to the U.S. power grid, the need for a multipronged approach for cyber deterrence is clear. In addition to *deterrence by denial*, U.S. cyber deterrence strategy includes a *deterrence by cost imposition* component that states,

> In accordance with rights established under international law, the United States Government reserves the right to use all necessary means—diplomatic, informational, military, and economic—to defend the nation and U.S. interests from malicious cyber activities. (White House, 2015, p. 10)

This broad range of deterrence responses requires a multi-agency approach. For instance, the U.S. Department of Treasury, in consultation with the Departments of Justice and State, is responsible for "sanction[ing] malicious cyber actors whose actions threaten the national security, foreign policy, or economic health or financial stability of the United States" (Monaco, 2015). DoD is specifically tasked with "creating credible and reliable options for the President to deter adversaries from attacking in cyberspace and to defend the nation from cyber attacks" (White House, 2015, p. 13).[1]

The Pentagon has recognized that any deterrence response must be conducted "in a manner consistent with U.S. and international

[1] In addition, the DoD Cyber Strategy states, "the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests" (DoD, 2015, p. 10).

law" (DoD, 2015, p. 2; see also White House, 2015). The Defense Science Board's 2017 cyber deterrence report echoed this sentiment: "In order to support timely decision-making, the 'plays' in this [cyber deterrence] playbook must be in the context of a clear policy and legal framework for their employment" (Defense Science Board, 2017, p. 14). In the deterrence context, a key consideration is the *jus ad bellum* framework under international law governing when retaliatory options are available. Such responses must comport with principles of international humanitarian law, which are also reflected in domestic laws and regulations. However, a lack of clarity in the application of international law and existing norms in cyberspace is a key challenge for understanding the available options for countering cyber aggression.

In this chapter, we aim to elucidate potential options for deterring the threat of cyberattacks on the power grid through the threat of cost imposition, as guided by international law. To do so, we provide a brief history of international agreements on the law of war, discuss international law and its implications for cyber deterrence, discuss available options for a cyber deterrence strategy, and then present conclusions on deterrence by cost imposition in cyberspace. Although not addressed in this report, domestic law and its implications will also be important determining factors for available deterrence options. Additionally, we do not assume in this report that nation-states will be compelled to follow international law. Rather, we provide a view of the bounds of international law as it pertains to cyber deterrence. Furthermore, although this chapter pays particular attention to deterring cyberattacks on the power grid—one section, for example, discusses potential deterrence mechanisms for the cases of the Russian threat to the U.S. and Ukrainian power grids—its implications are broader and help inform the conversation on cyber deterrence at large.

A Brief History of International Agreements Shaping the Law of War

From the First Geneva Convention, initially drafted in 1864, to the Chemical Weapons Convention enacted in 1997, international agreements have been convened to develop a shared understanding of the law of warfare. The history of international agreements has been motivated by the atrocities of wars past; the Geneva Conventions of 1949 notably responded to atrocities of World War II by taking key lessons from the Nuremberg trials. Here, we briefly highlight key developments in the history of international agreements on the law of war.

International agreements have focused on two key concepts: the right to war (*jus ad bellum*) and the law on conduct in war (*jus in bello*). The right to war provides legal criteria for when a country is justified to engage in war, and these criteria thereby provide a key guide to permissible options for cost imposition in a deterrence strategy. Although several international agreements touch on the right to war, it is largely governed by the Charter of the United Nations. The charter, signed in 1945, sets criteria on self-defense and the use of force, prohibiting the use of force unless in justified self-defense (United Nations, 1945), a topic discussed in detail in the next section.

The law on the conduct in war (often referred to as *international humanitarian law*) is largely governed by the Geneva Conventions. Ratified by 196 states in the wake of World War II, the four Geneva Conventions of 1949 represent the standard reference on international humanitarian law. Each of the four separate conventions has an objective. The first convention is a revision of the 1929 convention "for the amelioration of the condition of wounded and sick in armed forces in the field" (International Committee of the Red Cross, 1949). The second is a revision of the 1907 Hague convention "for the amelioration of the wounded, sick, and shipwrecked members of armed forces at sea." The third is a revision of the 1929 convention "relative to the treatment of prisoners of war." And the fourth is based on Hague convention IV of 1907 and is "relative to the protection of civilian persons in the time of war"; this convention is most acutely relevant to this

discussion. Building on previous revisions and followed by the addition of three protocols, the Geneva Conventions and agreements on international humanitarian law have been dynamic in responding to the evolution of conflict.[2]

Early international agreements addressed war on land and sea, and later agreements addressed the complications of war in the air and the use of modern weapons. Notably, the Biological Weapons Convention, signed in 1972, and the Chemical Weapons Convention, signed in 1993, were designed to supplement the Geneva Conventions by setting restrictions on new methods of conflict. More recently, after the 1998 signing of the Rome Statute, the International Criminal Court was implemented in 2002 and prosecutes "four core crimes": genocide, crimes against humanity, war crimes, and crimes of aggression (Arsanjani, 1999).

As conflict evolves and actions in cyberspace pose real risk to key intuitions, infrastructure, and the power grid, some have called for new agreements that adapt international law and norms to new challenges. At the 2017 RSA Conference (a series of large annual conferences of information technology security professionals named for the public-key encryption company RSA Data Security), Brad Smith, the president of Microsoft, called for a new "Digital Geneva Convention" (B. Smith, 2017). He noted that a rise in nation-state aggression in cyberspace has led to peacetime attacks on civilians that run contrary to the spirit of the Geneva Conventions, resulting in a need for new agreements.

The call for new international agreements is not new. In 2009, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan organized to form the Shanghai Cooperation Organization in an effort to reach agreement on information security (Droege, 2012). In 2011, Russia proposed new agreements on cyber norms—an "International Information Security Code"—to the United Nations (Droege, 2012).

---

[2] The Geneva Conventions of 1949 were modified through the addition of protocols. Protocol I, for the "Protection of Victims of International Armed Conflicts," was added in 1977; Protocol II, for the "Protection of Victims of Non-International Armed Conflicts," was added in 1977; and Protocol III, for the "Adoption of an Additional Distinctive Emblem," was added in 2005. See also Webster, 2011.

More notably, the Tallinn Manual—which is a mostly academic review of international law in the context of cyber war and was originally convened in 2009 by the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence—is the largest exploration of the topic. However, until new agreements are made, historical agreements, existing norms, and international law provide the most insight into permissible actions in cyberspace. The next section takes a look at existing law and norms to elucidate opportunities for deterrence in cyberspace.

Cyber Deterrence Under International Law

International legal experts agree on general principles that govern retaliatory responses to cyberattacks on critical infrastructure, including the power grid, many of which are articulated in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Schmitt, 2017). However, there remains disagreement about how these principles apply under specific circumstances, and the law continues to evolve based on these debates and on state practice (see Schmitt, 2014). This section presents an approach for identifying retaliatory options for a cyberattack on the power grid under a permissive view of these applicable principles.[3]

Broadly speaking, international law requires retaliatory responses to be proportional to the hostile act. There are three general categories of retaliatory responses to cyberattacks: self-defense, countermeasures, and retorsions. The availability of each depends largely on two factors: the severity of the attack and the extent to which the attack may be attributed to a state. Retaliatory options are broadest when a state is the victim of a destructive or highly disruptive cyberattack that is attributable to another state. Conversely, options are most narrow when a cyber operation produces little or no physical consequences or is launched by a nonstate actor that has limited connection to a state.

[3] We note instances in which there is disagreement among scholars and experts with the approach presented.

The Right to Self-Defense Against Harmful Cyber Operations

The right of *self-defense* enables a state to use military force—which can include both cyber and kinetic operations—against an aggressor. Self-defense provides the most robust array of deterrence options and thus is available in response to only the most harmful types of cyber operations.

The Severity Requirement for Self-Defense

According to the United Nations Charter, a state may use force in self-defense only if it is subject to an "armed attack," which has two requirements.[4] First, the attack must be an illegal "use of force." Legal experts continue to debate what precisely constitutes a "use of force" in the cyber context and recommend weighing the following nonexhaustive factors: severity, immediacy, directness, invasiveness, measurability of effect, military character, state involvement, and presumptive legality (Schmitt, 2017, Rule 70, para. 9). These factors still leave significant ambiguity regarding what constitutes use of force in the cyber domain. Yet, it is apparent that any cyber operation that results in loss of life or the significant degradation of performance of electric power infrastructure is likely to qualify as a use of force.

Second, it is necessary to distinguish "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" (ICJ, 2003, p. 187).[5] A harmful cyber operation may sat-

---

[4] See United Nations, 1945, Articles 2(4) (prohibiting the use of force) and 51 (carving out a self-defense exemption to this prohibition "if an armed attack occurs").

[5] The gravity requirement for armed attacks comes from International Court of Justice (ICJ) rulings against the United States. In *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)* (ICJ, 1986), the United States attempted to justify its use of force against Nicaragua as collective self-defense of Costa Rica, El Salvador, and Honduras from attacks by Nicaraguan bands (para. 126). The ICJ rejected this argument and ruled that Nicaragua's actions against its neighbors were "frontier incidents" that did not meet the gravity threshold for an armed attack triggering the right of self-defense (para. 292(2)). The ICJ reaffirmed the distinction in *Case Concerning Oil Platforms (Iran v. United States of America)* (ICJ, 2003, para. 51), where it concluded that Iranian missiles and mines that damaged U.S. vessels did not constitute an "armed attack" that justified the United States destroying two offshore oil platforms from which the attacks were launched. See also ICJ, 2005, para. 147. Despite these rulings, the United State continues to "take the position that the inherent right of self-defense potentially applies

isfy the gravity requirement for an armed attack if it causes physical destruction, death or injury to persons, or severe disruption to critical infrastructure, such as a major power outage. There is debate regarding whether nondestructive but disruptive attacks may constitute armed attacks. The United States has endorsed the view that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack," (United Nations Secretary-General, 2011, p. 18). Additionally, Li, 2013, has argued in support of that view (using the analogy of naval blockades to argue that nondestructive cyberattacks causing severe economic disruption may constitute an armed attack). The editor and principal author of the Tallinn Manual, Michael N. Schmitt, has argued that the armed attack must involve the "causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects" (Schmitt, 2011, p. 588). Schmitt, however, predicts that the law will evolve to allow nondestructive cyberattacks to qualify as armed attacks. In a later work, Schmitt states that, although

> the law of self-defense has not quite evolved to the point where non-destructive or non-injurious cyber operations can quality as armed attacks[,] . . . it is almost certain that states will begin to treat such cyber operations as armed attacks to which they can respond forcefully when the consequences are sufficiently severe. (Schmitt, 2014, p. 283)

While the United Nations Charter notes that a state may use force in self-defense only if it is subject to an "armed attack," this could be moderated by others to allow for preemption. Under the doctrine of

---

against *any* illegal use of force," regardless of severity (DoD, Office of General Counsel, 2016, para. 1.11.5.2, emphasis added). This position, however, is not widely held outside of the United States—or even among U.S. experts outside of government. See Waxman, 2017, which presents the gravity requirement as settled law in Senate testimony. See also Schmitt, 2014, pp. 284–285, in which the author (a U.S. Naval War College professor) explains that the "U.S. stance . . . made sense for states that wielded significant [conventional] military power," but he predicts that the stance "is liable to weaken over time" in the cyber context because the "relative impunity afforded by [conventional] military superiority . . . dissipates significantly in cyberspace."

anticipatory self-defense (preemption), a state need not wait until the cyber armed attack has occurred but may undertake self-defense measures if there is credible evidence that such an attack is imminent.[6] An armed attack is imminent if the aggressor has the requisite intent and capability and the last window of opportunity to prevent the attack through peaceful means has passed (Schmitt, 2017, Rule 73, para. 2).

Given the requirements of the Geneva Conventions, it is important to emphasize that measures taken in self-defense must be necessary and proportional. The necessity principle permits self-defense only if alternative measures are insufficient to defeat a threat; that is, self-defense is not necessary if a cyberattack may be thwarted through passive defenses. And proportionality limits the scale and scope of self-defense to what is needed to defeat the threat. This does not limit self-defense to the same mode as the aggression—kinetic measures may be used in response to a cyber armed attack, and vice versa—but a massive retaliatory response against a comparatively minor attack is prohibited.[7] And, finally, measures taken in self-defense must comport with laws of armed conflict, which include treaty-based and customary rules concerning military need, distinction, and proportionality (Schmitt, 2017, Rule 15; see also International Law Commission, 2001, Article 4).

The Attribution Requirement for Self-Defense

For the use of force undertaken in self-defense to be necessary and proportional, it must at least be directed toward the responsible actors. When a cyber-armed attack (a cyberattack reaching the level of armed attack) may be traced to "organs of a State, or persons or entities empowered by domestic law to exercise elements of government authority," that state may be held responsible and may be the legitimate target of necessary and proportional self-defense measures (Schmitt, 2017, Rule 15; see also International Law Commission, 2001, Arti-

[6] The Israeli attack on Arab armies in the Six-Day War is often cited as the quintessential example of anticipatory self-defense.

[7] See ICJ, 2003, para. 77. The ICJ found that U.S. destruction of two Iranian oil platforms (used as radar sites) and several vessels and aircraft was not a proportional response to the mine attack on a U.S. frigate that caused no loss of life.

cle 4). And a cyber-armed attack committed by a nonstate actor may be legally attributed to a state if the state that instructed the nonstate actor to launch the attack exercises "effective control" over the nonstate actor (Schmitt, 2017, paras. 7–8). The instruction-or-control test is stringent and does not make a state responsible—and thereby a legitimate target of self-defense—simply by supporting the nonstate actor (e.g., by supplying financial resources).

Under certain circumstances, a cyberattack victim may use force in self-defense directly against a responsible nonstate actor located in a host state, even if the host state cannot be held responsible for the attack. Due care must be taken to respect the sovereignty of the host state, which holds primary responsibility for preventing groups from launching harmful cyber operations from within its territory. Thus, the victim may launch self-defense measures into the territory of the host state only if the host is unwilling or unable to discharge the responsibility. The "unable or unwilling" doctrine is an extension of necessity; if the host state were capable of ending the threat, self-defense would be unnecessary (Deeks, 2012). The doctrine is supported by state practice outside of the cyber context. For instance, the 2001 U.S. invasion of Afghanistan was justified, in part, based on the Taliban regime's unwillingness to prevent al Qaeda from using its territory as a base of operations (Negroponte, 2001).

Countermeasures Against Cyber Operations Below the Armed Attack Threshold

When a state is subject to a cyberattack that falls short of an armed attack, it may not invoke the right to self-defense. But it may employ *countermeasures*, which are defined as otherwise unlawful acts that may be undertaken by an injured state in response to another state's intentionally wrongful conduct (International Law Commission, 2001). For the purpose of cyber deterrence, countermeasures could come from responsive force by cyberattack (Hathaway et al., 2012).

The Severity Requirement for Countermeasures

A countermeasure may be undertaken only in response to an intentional wrongful act. In the cyber context, any interference with

electricity infrastructure is likely to qualify. At the very least, such operations violate the sovereignty of another state. There remains disagreement regarding the legality of cyber espionage. A majority believe that remotely accessing and exfiltrating sensitive data, by itself, violates no international law (Schmitt, 2017, Rule 32, para. 8).[8] But if such access and exfiltration requires physical or digital intrusion—for example, through "the insertion of a USB flash drive into a computer" (Rule 32, para. 9) or "emplacing malware into a system" (Rule 4, para. 14)—sovereignty is violated and, therefore, countermeasures may be imposed.

Countermeasures must be proportional to the wrongful act and generally must not involve the use of force. But some scholars and jurists believe that countermeasures constituting a limited use of force (also called *reprisal*) are lawful in response to an intentional wrongful act that itself was an unlawful use of force.[9] Under the permissive view of deterrence presented in this report, a state subject to a cyberattack amounting to a "less grave" use of force—that is, one that measurably degrades the operation of the electricity infrastructure but not enough to trigger the right of self-defense—may respond with a forcible reprisal. But, again, such reprisals must be proportional to the attack and fall "within [a] more limited range and quality of responses" in comparison to self-defense measures (ICJ, 2003, p. 333, para. 13 of Judge Simma's dissent). In practical terms, this likely means that reprisals for cyberattacks against the power grid should involve only cyber counterattacks rather than kinetic options.

If the cyberattack against electricity infrastructure does not amount to a use of force—for example, installation of surveillance malware—any responsive countermeasure must also be nonforceful.

---

[8] A minority believe that legality of such acts depends on the sensitivity of the data breach. For instance, "exfiltration of nuclear launch codes" via cyber means was deemed illegal under the minority view (Schmitt, 2017).

[9] See ICJ, 2003, p. 333, para. 13 of Judge Simma's dissent, which recognizes that, although the general right of self-defense is not permitted against "less grave" uses of force, "Against such hostile acts, a State may of course defense itself, but only within the more limited range and quality of responses." See also Bowett, 1972, which finds that, although reprisals are *de jure* illegal, they are *de facto* accepted when proportional.

A proportional countermeasure may involve a counter cyberattack that installs malware on the aggressor's computer networks. Of course, countermeasures need not be symmetrical; a victim state may, for instance, suspend trade or investment protections.

The Attribution Requirement for Countermeasures

Only states owe each other obligations under international law; therefore, countermeasures taken in response to a breach of such obligations require evidence of state responsibility. Nonetheless, cyber countermeasures may be employed to target responsible nonstate actors under two scenarios.

First, as in the self-defense context, the conduct of a nonstate group may be attributed to a host state if that state instructs or exerts "effective control" over the group. The injured state may treat the host state as responsible for breaching an international obligation and impose countermeasures in response. The countermeasures may target either the host state or responsible nonstate groups located therein (Schmitt, 2017).

Second, cyber countermeasures may target the responsible nonstate group in cases in which the host state fails to undertake reasonable efforts to stop the attack. Even if the host state cannot be held responsible for the cyberattack, it can breach its legal obligation to prevent that attack from being launched from within its territory or through its digital infrastructure. Under this scenario, the countermeasure is not imposed on the nonstate group—it merely targets that group. Rather, it is imposed on the host state for unlawfully acquiescing to or supporting harmful cyber operations launched from within its territory (Schmitt, 2017).

This concept is similar to the self-defense test against nonstate actors, with one key difference. Whereas self-defense is permitted when the host state is "unwilling or unable" to prevent armed attacks by the nonstate group, countermeasures are permissible only if the host state is merely "unwilling" to do so. This standard is met when the host state actively supports the nonstate group—even if such support falls short of the "effective control" standard needed to hold the host state directly responsible. But countermeasures may not be imposed when the state

undertakes a reasonable, good-faith effort to stop the nonstate actor but is unable to do so.

Retorsions

The final category of retaliatory responses consists of *retorsions*, which are legally permissible but unfriendly acts. For instance, the United States imposed economic sanctions and expelled diplomats following alleged Russian cyber operations aimed at interfering in the 2016 presidential election (Obama, 2016). Such indisputable retorsions are important components in the United States' broad-range approach to cyber deterrence, which includes law enforcement, economic, diplomatic, and military measures (White House, 2015). Because retorsions are always legal under international law, they can be imposed regardless of the severity of a cyberattack or whether a state can be held directly responsible.

Options for Deterring Actions in Cyberspace

The threat of retaliation could be an effective tool in a strategy aimed at deterring cyberattacks on the power grid. Although, in this report, we do not seek to recommend the best retaliatory options, we do aim to provide insight on which options are available. The availability of these options is largely governed by the law of self-defense and the law of countermeasures. The right of self-defense offers the broadest range of punitive response options, potentially including offensive cyber and kinetic responses against state and nonstate actors. However, such responses are available only when faced with the "most grave" cyberattacks that satisfy the gravity requirement for armed attack. When facing a "less grave" cyberattack, the injured state may impose countermeasures. Such countermeasures may involve limited cyber counterattacks that do not amount to a "use of force" targeting the responsible state or nonstate actor. And an intermediate option may be available when the original cyberattack qualifies as a use of force but not an "armed attack." In such cases, a cyber reprisal comprising a more forceful but proportional cyber-counterattack may be permitted.

Table 3.1 maps the afore-mentioned cost imposition options. The vertical categories, from top to bottom, represent the objects of attribution:

- a state actor
- a nonstate actor under state control or direction
- a nonstate actor with little or no state support.

Although the legal attribution need not be foolproof, it must be based on reasonable evidence. The technical challenges of cyberattack attribution could inhibit the ability to retaliate. The horizontal catego-

Table 3.1
Cost Imposition Options

	Severity (Intended or Actual) →		
Attributed Actor	**Less Than Use of Force**	**Use of Force**	**Armed Attack**
State actor	Nonforceful countermeasures (including cyber counterattacks)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks)	Use of force in self-defense against the state
Nonstate actor under state control or direction	Nonforceful countermeasures (including cyber counterattacks targeting the state or nonstate actor)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks targeting the state or nonstate actor)	Use of force in self-defense against the state or nonstate actor
Nonstate actor with little or no state support	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Use of force in self-defense against the nonstate actor *only if* the host state is unwilling or unable to prevent attack

NOTE: In this table, we consider limited reprisals under the broad definition of deterrence.

ries in Table 3.1, from left to right, denote increasing severity of the cyberattack:

- an unlawful intervention (less than use of force)
- a "less grave" use of force
- an armed attack (i.e., a "most grave" use of force).

Importantly, the "use of force" and "armed attack" thresholds remain ill-defined in the cyber context—and indeed they are incomplete even in the noncyber *jus ad bellum* framework. The United States therefore has discretion to advance its own definition within a space of reasonable debate.

The matrix in Table 3.1 provides an overview of options for cost imposition that could be included as part of a broader deterrence strategy. The options presented help elucidate which means and measures could be used in a cyber deterrence strategy dependent on the attack severity, strength of attribution, and type of actor. Table 3.1 does not include retorsions, which are always available.

When we read the table from left to right, the available options grow as the severity intensifies. For example, consider a cyberattack attributed to a state actor: If the attack does not meet the criteria for use of force, then countermeasures are available but may not rise to the use of force. However, if the attack does meet the criteria for use of force, then both nonforceful countermeasures and limited reprisals against the responsible state are allowed. Furthermore, if the cyberattack is considered an armed attack, self-defense measures may be undertaken, provided the measures adhere to principles of necessity and proportionality. As the attribution shifts downward from a state actor to a nonstate actor, retaliations are allowed against the nonstate actor with state support or against the host state if that support amounts to direction or control. But without such evidence showing that the nonstate actor is essentially an extension of the state, retaliatory options become more limited. If a largely independent nonstate actor launches a cyber-armed attack, self-defense measures may be directed toward that actor only if the host state is unable or unwilling to stop the attack. If the cyberattack from an independent nonstate actor falls short of armed attack, then retali-

ation (1) is impermissible where the host state makes reasonable efforts to halt the malicious activities and (2) may not amount to a use of force. The cost imposition options outlined in Table 3.1 do not provide a legal path to retaliation when attacks lack confident attribution.

The result is that attacker type, attack severity, and the confidence of attribution will largely guide which punitive measures (e.g., use of force, nonforceful countermeasures, and limited reprisals) are legally permissible under international law. Confident attribution, however, remains a challenge. Some reports, such as the Office of the Director of National Intelligence's 2017 report assessing Russian cyber actions during the 2016 U.S. presidential election (Office of the Director of National Intelligence, 2017), have therefore taken to expressing varying levels of confidence associated with their findings. Furthermore, with attribution findings coming from various sources, ranging from private firms to government agencies, Davis et al., 2017, and others have suggested creating a nongovernmental body designed for the sole purpose of creating credible and confident attribution free from conflicts of interests. Currently, expressing confident and credible attribution is not a guarantee in all scenarios. The options for cyber deterrence through cost imposition are, thus, unsurprisingly and highly dependent on each scenario.

In the next two sections, we discuss potential responses under international law to two real-world cyber operations targeting the power grid. First, we consider the penetration of U.S. energy grid networks by Russian government hackers and exfiltration of industrial control system information. Because this operation amounts to little more than espionage, retaliatory options are relatively limited. Second, we consider the Russian cyberattack disrupting industrial control systems and causing widespread blackouts in Ukraine. This type of serious disruption arguably triggers a state's right to use military force, either as a limited reprisal or in self-defense.

The Russian Cyber Penetration of the U.S. Power Grid

A March 2018 US-CERT report concluded, "Since at least March 2016, Russian government cyber actors . . . targeted government entities and multiple U.S. critical infrastructure sectors" (US-CERT, 2018). Nota-

bly, the hackers "gained access into energy sector networks" by using malware, phishing, and other techniques to obtain network credentials (US-CERT, 2018). Once inside the networks, the hackers "conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems" (US-CERT, 2018). Nothing in the US-CERT report indicated that functionality of the power grid was degraded as a result of the cyber intrusions, but some defense experts expressed concern that the intrusions might enable the hackers to "plac[e] the tools that they would have to place in order to turn off the power" (Naylor, 2018).

What deterrence responses are available in response to such intrusions? As an initial matter, legal attribution does not appear to be an issue because US-CERT, 2018, identified the responsible parties as "Russian government cyber actors." The hacks were therefore legally attributable to Russia, and any response may be directed toward Russia or the government actors themselves. However, the scope of permissible responses is limited because network surveillance and information collection are commonplace acts of espionage that do not give rise to robust options. Such activities do not amount to an armed attack that triggers the United States' right to self-defense because those activities did not cause any physical destruction or disruption of services. The attacks did constitute unlawful interference in U.S. sovereignty because the hackers placed surveillance malware into U.S. networks. In the matrix of cost imposition options, this case fits squarely within the upper left: an attack attributed to a nation-state not rising to the level of use of force; see Table 3.2.

Nonetheless, the right of *anticipatory* self-defense warrants discussion because the vulnerabilities exposed may enable Russia to launch a disruptive cyber operation that rises to the level of an armed attack. Indeed, Russia has demonstrated the ability to use cyberattacks to cut electricity to hundreds of thousands of Ukrainians (see the following section). If the intrusions were the initial phase of an *imminent* cyberattack of similar scope and scale, the United States need not wait for the final phase (e.g., delivery of a virus that shuts down power) before responding in anticipatory self-defense. The question is whether there exists concrete evidence that Russia, in fact, intends to severely dis-

Table 3.2
Area of Cost Imposition Options for the Russian Cyber Penetration of the U.S. Power Grid

	Severity (Intended or Actual) →		
Attributed Actor	**Less Than Use of Force**	**Use of Force**	**Armed Attack**
State actor	Nonforceful countermeasures (including cyber counterattacks)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks)	Use of force in self-defense against the state
Nonstate actor under state control or direction	Nonforceful countermeasures (including cyber counterattacks targeting the state or nonstate actor)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks targeting the state or nonstate actor)	Use of force in self-defense against the state or nonstate actor
Nonstate actor with little or no state support	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Use of force in self-defense against the nonstate actor *only if* the host state is unwilling or unable to prevent attack

NOTE: In this table, we consider limited reprisals under the broad definition of deterrence.

rupt the power grid and whether the last window of opportunity to take preemptive actions has passed. In this case, the US-CERT, 2018, report did not indicate that a Russian attack to disrupt the power grid was imminent. Without credible evidence of an imminent threat, DoD is unable to take retaliatory actions under the theory of anticipatory self-defense.

With self-defense off the table, the United States is entitled to impose countermeasures in response to cyber operations that violate an international obligation. Espionage and surveillance generally do not violate international law unless the underlying methods are unlawful. Some of the cyber surveillance methods that Russia employed amounted to open-source collections that presented no obvious legal

problems. For instance, US-CERT reported that Russian agents "downloaded a small photo from a publicly accessible human resources page," which, "when expanded, was a high-resolution photo that displayed control systems equipment models and status information in the background" (US-CERT, 2018). But other methods were unlawful. Surveillance using vehicles that violate a state's airspace or territorial waters infringe upon sovereignty. By analogy, Russian surveillance using malware introduced clandestinely into computer networks physically located within a state's territory also constitutes a violation of sovereignty.

Accordingly, Russia's cyber intrusions into U.S. computer networks were unlawful and entitle the United States to impose proportional countermeasures. Such countermeasures may include cyber counterattacks and need not be necessary to defeat or prevent Russia's unlawful cyber intrusion. Rather, the countermeasures should be imposed with the aim of convincing Russia to halt its intrusions into U.S. cyber infrastructure. Such countermeasures may not include forceful reprisals over cyberspace, because the Russian hacks did not rise to even a "less grave" use of force: There was no evidence that the U.S. power grid lost functionality in a measurable way as a result of the intrusions.

The 2015 Russian Cyberattack Against the Ukrainian Power Grid

On December 23, 2015, power stations operated by Ukrainian electricity companies became disconnected from the power grid, and approximately 225,000 customers were left without power (Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, 2016; Dragos, 2017). The outage was caused by hackers who illegally accessed the company's networks, performed months of reconnaissance, and eventually took remote control of the supervisory control and data acquisition systems (Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, 2016; Greenberg, 2017a). Ukraine immediately attributed the attack to "Russian security services" (Polityuk, 2015), and independent experts confirmed that the attacks were carried out by a Russian hacker team known as "Sandworm" (Greenberg, 2017b). Ukrainian operators

manually restored power after approximately six hours, but that effort required wiping systems and destroying compromised devices, which left operators without automated control of power distribution for about a year (Dragos, 2017). Russian cyber actors have since launched additional cyberattacks disrupting the Ukrainian power grid, notably in December 2016 and June 2017 (Dragos, 2017).

The December 2015 Russian cyberattack on the Ukrainian power grid went beyond simple acts of exploration and provides a useful case for understanding cost imposition options within a deterrence strategy. We use this subsection to analyze how retaliation could have occurred. To do so, we consider the cyberattack as an isolated incident—that is, separate from the follow-on attacks and the wider context of the Ukrainian-Russian conflict since Russia annexed Crimea in 2014. This approach provides a more relevant scenario for Pentagon planners—essentially what might have happened if the Russian actors had exploited vulnerabilities to take actions on the U.S. power grid.[10] The December 2015 electricity disruption in Ukraine could be categorized as an armed attack under a more flexible definition of that term. But, arguably, it did not trigger the right of self-defense, because power was restored relatively quickly—and, hence, the necessity requirement was not satisfied. Nonetheless, the attack was an unlawful use of force, against which countermeasures could have been imposed. Under an expansive view of deterrence, such countermeasures could have included forceful but proportional cyber reprisals if the Russian government were held accountable.

The first question is whether the electricity disruption constituted an armed attack that is a conditional precedent for self-defense. Some international law experts believe that a cyberattack must cause physical destruction or injury before rising to the level of an armed attack (see general legal discussion in the section on Cyber Deterrence Under International Law). There is no indication that the December 2015

[10] Although we specifically note Pentagon planners, under current policy, DoD is not alone in taking punitive actions. Others, including the Department of State, Congress, and the White House, are key stakeholders in decisionmaking for cyber retaliation.

cyberattack caused any such effects, so, under that rubric, Ukraine was not entitled to use force in self-defense.

A competing view, however, is that severe disruption of critical infrastructure functions can amount to an armed attack (see, for example, Graham, 2010). There is little doubt that the power grid qualifies as critical infrastructure, so the issue is whether disabling power stations and causing the loss of power to several hundred thousand people is sufficiently severe. In making this assessment, it is worth noting that the victim state's mitigation efforts cannot demote the severity of the attack; for instance, a missile strike that fails to damage sheltered targets is still an armed attack. Thus, the fact that manual operators were able to restore power after six hours does not mean that that is the relevant duration of a severity analysis. Rather, the restoration effort required wiping the automated control system because it was permanently compromised. The cyber weapon deployed was not designed to restore functions after a certain time had passed but rather to render the target systems indefinitely inoperable.[11]

In the end, a coordinated attack disabled several power stations and left hundreds of thousands of Ukrainians without power in the middle of winter but did not produce any physical destruction. A physical weapon that would produce a similar effect is the electromagnetic pulse (EMP) weapon that can disable electronics without causing structural damage.[12] Had such weapons been detonated near Ukrainian power stations, there would be no question that an armed attack had occurred.[13] Accordingly, there is a strong argument that the December

---

[11] That said, reparability is one of the nonexhaustive factors that experts identified in the Tallinn Manual as being relevant for determining the seriousness of an attack. Here, the power grid was repaired relatively quickly, but the affected networks and systems arguably were not reparable because they had to be wiped clean, replaced, or both.

[12] In August 2018, the Air Force's Counter-Electronics High-Powered Advanced Missile Project successfully tested an EMP missile capable of disabling electronics without causing structural damage (see Lewis, undated).

[13] Because hardware and software must be replaced, it might be more difficult to restore functions after an EMP attack; thus, the analogy is not perfect. But reparability and mitigation fall more naturally as part of the necessity discussion (see later in this chapter) rather than as factors for armed attack.

2015 cyberattack against the Ukrainian power grid satisfies the "severe disruption" element under the more flexible definition of an armed attack. In the matrix of deterrence options from Table 3.1, this would put the attack in the upper-middle section as a nation-state attack representing an armed attack or use of force. However, uncertainty persists when a cyber operation that constitutes the attack rises to an armed attack, as well as when attribution to Russia is uncertain. As a result, Table 3.3 displays a fuzzy area of options shown within the oval.

In addition to satisfying the armed attack requirement, Ukraine must comply with necessity and proportionality requirements. The necessity principle prohibits the use of force in self-defense when nonforceful measures, such as mitigation, may defeat aggression. Here, the restoration of power after six hours plays a key role in assessing neces-

Table 3.3
Area of Cost Imposition Options for the 2015 Russian Cyberattack on the Ukrainian Power Grid

	Severity (Intended or Actual) →		
Attributed Actor	**Less Than Use of Force**	**Use of Force**	**Armed Attack**
State actor	Nonforceful countermeasures (including cyber counterattacks)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks)	Use of force in self-defense against the state
Nonstate actor under state control or direction	Nonforceful countermeasures (including cyber counterattacks targeting the state or nonstate actor)	Nonforceful countermeasures or limited reprisals (including cyber counterattacks targeting the state or nonstate actor)	Use of force in self-defense against the state or nonstate actor
Nonstate actor with little or no state support	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Nonforceful countermeasures *only if* the host state is unwilling to make a reasonable effort to prevent attack	Use of force in self-defense against the nonstate actor *only if* the host state is unwilling or unable to prevent attack

NOTE: In this table, we consider limited reprisals under the broad definition of deterrence.

sity. Although self-defense to defeat a cyber-armed attack on the power grid could include a counterattack, such as a "hack back," that is meant to disrupt the ongoing cyberattack, relatively quick restoration meant that self-defense was not necessary to defeat the armed attack. Similarly, a highly resilient power grid that minimized the effect of a disruption could also undercut the necessity justification for self-defense. But resilience and effective mitigation do not forever tie the victim state's hands. If the electricity disruption were not a one-time incident but persistent or periodic—as is the case with Russian attacks against the Ukrainian power grid—it may become necessary for the victim to act in self-defense to end those attacks.

The proportionality requirement requires Ukraine to use the minimum force necessary to defend itself. Proportionality generally favors responding to cyberattacks with cyber counterattacks because such responses are less destructive and symmetrical to the aggression. And the responsible group, Sandworm, is the natural target. But if "the source of the cyber armed attack is relatively invulnerable to cyber operations," proportionality "would not preclude kinetic or cyber defensive operations against other targets in an effort to compel the attacker to desist" (Schmitt, 2011). If the Russian government were legally responsible—that is, by directing or controlling Sandworm—then self-defense measures could be directed against a broad range of Russian targets, including Russia' digital infrastructure. If Russian ties to Sandworm fall short of direction or control, Ukraine's self-defense measures may still target Sandworm because Russia is "unable or unwilling" to stop the attacks. But Ukraine could not legally target Russian infrastructure generally.[14]

Even if self-defense were not a lawful option, Ukraine could still impose countermeasures. There is little doubt that shutting down power to hundreds of thousands of people—even for a few hours—was an illegal use of force. If Russia were legally responsible, it breached an obligation to not use force, and Ukraine may respond with proportional countermeasures. Because a use of force is a significant breach,

[14] Israeli attacks against Lebanese infrastructure during the 2006 Lebanon War were criticized as disproportional to the need of self-defense against Hezbollah (see Kattan, 2006).

the appropriate countermeasures may be quite robust. Indeed, some scholars and jurists contend that a victim state may resort to the use of force as a countermeasure in such circumstances (see ICJ, 2005). Under this view, proportional cyber counterattacks against Russian networks may be permitted. But if Russia could not be held responsible as having directed or controlled Sandworm, it could not have breached the obligation to not use force. Russia would still have breached its obligation to prevent attacks from being launched in its territory, and Ukraine may have the right to impose countermeasures based on Russia's unwillingness to stop Sandworm. But the scope of such countermeasures would be more limited and could not encompass the use of force.

The United States does not have strong retaliatory options against an attacker that penetrates the power grid network and exfiltrates sensitive data. But if the attacker takes one step further and uses the stolen data to design and deliver malware that disrupts the power grid, causing substantial loss of power, retaliatory options are much broader. In practice, however, it is not always possible to tell the difference, because penetration and surveillance are necessary first steps toward power disruption. During a period of high tension, espionage and surveillance may be mistaken as precursors to a widespread disruption. The potential for misunderstanding and unintentional escalation is great, especially in the absence of a transparent deterrence policy.

Toward a Strategy for Deterrence by Cost Imposition

Through the analysis in in this chapter and within Table 3.1 in particular, we begin to develop options for using cost imposition measures to deter cyber aggression against the power grid. Although we use international law to guide the construction of these options, domestic law, regulations, and policy may further guide the options.

However, we also find reason to believe that considerable uncertainty on cost imposition is likely. For one, the Cyber Deterrence Under International Law section highlights the ambiguity of classifying a cyberattack as a use of force or armed attack. Efforts to ameliorate confusion may enhance the strength of deterrence by adding

clarity to cost imposition, and the importance of these criteria was underscored by Schelling, 1981. Furthermore, uncertain attribution in cyberspace remains an issue that undermines deterrence (Baliga, de Mesquita, and Wolitzky, 2019; B. Edwards et al., 2017). Although proposals to enhance attribution in cyberspace have been made (e.g., Davis et al., 2017), DoD efforts to strengthen credible attribution could work to enhance the cyber posture of the United States and the strength of deterrence. Furthermore, it may also work against deterrence to not have greater clarity on whether cyber aggression on the power grid carries the threat of legal countermeasures, cyber countermeasures, or the full force of the military. The solutions to each area of uncertainty are multifaceted and span matters of technology, law, policy, and strategy.

If adversaries believe that aggression will be followed by only low-level cost imposition, deterrence could be undermined. Perhaps worse, uncertainty could lead to unintended escalation. In the current case of Russian aggression against the U.S. power grid, the United States could potentially interpret Russian movements in cyberspace as representative of an imminent attack while Russia views its own movements as routine espionage. It is therefore feasible that a cyberattack representing an imminent use of force could be responded to with a military strike using kinetic force, escalating the confrontation into a new domain.

Although aggression in the cyber domain presents new challenges for international law and thus deterrence, options for cost imposition remain the same. Depending on the adversary and the severity of the attack, the U.S. government and DoD will face the decision of how to respond—with or without force, within the cyber domain or not. The options presented in this discussion can aid DoD in articulating the threat of cost imposition.

CHAPTER FOUR

Conclusion

This report explored two approaches for deterring attacks against the U.S. power grid in a world of increasing cyber aggression: enhancing resilience and reliability to deter by denial and using the threat of retaliation to deter by cost imposition. The report is a first step, exploring how both approaches lead to options for inclusion in a broader deterrence strategy. These two approaches are not substitutes; they are complementary to each other and to other defense strategies.

We are not the first to recommend these strategies. The contribution of this report is to help develop frameworks and context to support DoD decisionmaking regarding both deterrence by denial and deterrence by cost imposition. For deterrence by denial, we focused on outside-the-fence interventions—ways in which DoD can engage with entities or infrastructure not owned by DoD. We identified three broad categories of outside-the-fence interventions: shifting the fence line, influencing governance, and leveraging resources. We then identified factors that seem to affect the ease of implementation of these various types of interventions: ownership, relationships, and laws and regulations. Case studies show that outside-the-fence interventions complement rather than replace existing inside-the-fence interventions and that resilience and reliability interventions can offer important secondary benefits in addition to their deterrence value. Improving resilience and reliability can enhance DoD's ability not only to deter attacks by a military adversary but also to sustain operations under a broader set of potential perils, such as natural disasters, aging infrastructure, and other types of intentional harm to the power grid.

Furthermore, by exploring the applicability of international agreements on the law of war, we discussed options for deterring cyberattacks through the threat of cost imposition. For cyberattacks on the civilian electric power grid, we find that the severity of the attack and the strength of attribution reveal several options for retaliation. Cyber intrusions on the grid launched by nation-states, for example, may be countered with legal countermeasures. Attacks reaching the level of use of force could potentially warrant stronger responses through cyber means, while attacks reaching the level of armed attack could warrant military responses. In this framing, we find that the recent cyber intrusion into the U.S. power grid by Russian state actors would most likely fit the criteria of cost imposition through legal countermeasures, and the recent Russian cyberattacks on the Ukrainian power grid could be met with cyber countermeasures and perhaps a military response.

However, one challenge for deterrence comes from the ambiguity of cyberspace. We find that this ambiguity cuts in two key directions: cyberattack attribution and cyberattack severity. The problem of attribution is well known: It leads to unavoidable challenges in retaliating against attacks and, as a result, risks undermining deterrence. The ambiguity surrounding severity may lead to less-obvious problems; we find reason for concern that a lack of clarity on the meaning of use of force in cyberspace could produce unintended escalation. That is, cyber activity on the power grid that fits well within one country's definition of espionage could be interpreted by another country as an imminent attack leading to military retaliation and unintended escalation.

The exploration of deterrence options in this report opens several questions for future work. For example, future analyses could further explore the optimality of different resilience strategies and their contributions to deterrence by denial. Similarly, future analyses could evaluate the strategic benefit of the deterrence by cost imposition options discussed in this report.

References

AFRI—*See* Air Force Research Institute.

Air Force Research Institute, "Thor: Theater History of Operations Reports," webpage, undated. As of July 15, 2019:
http://www.au.af.mil/au/afri/thor/#.XS3H8S3MxTY

American Public Power Association, *U.S. Electric Utility Industry Statistics*, Arlington, Va., 2015.

American Water, "American Water Military Services Group," webpage, undated. As of September 27, 2018:
https://amwater.com/corp/products-services/military-services

Andres, Richard B., and Hanna L. Breetz, *Small Nuclear Reactors for Military Installations: Capabilities, Costs, and Technological Implications*, Washington, D.C.: National Defense University, Institute for National Strategic Studies, 2011.

Arsanjani, Mahnoush H., "The Rome Statute of the International Criminal Court," *American Journal of International Law*, Vol. 93, No. 1, 1999, pp. 22–43.

Baliga, Sandeep, Ethan Bueno de Mesquita, and Alexander Wolitzky, "Deterrence with Imperfect Attribution," working paper, February 12, 2019.

Barnes, Greg, "Chemical in Fayetteville's Tap Water May Cause Cancer," *Fayetteville Observer*, June 27, 2018.

Berman, Eli, Jacob N. Shapiro, and Joseph H. Felter, "Can Hearts and Minds Be Bought? The Economics of Counterinsurgency in Iraq," *Journal of Political Economy*, Vol. 119, No. 4, 2011, pp. 766–819.

Bowett, Derek, "Reprisals Involving Recourse to Armed Force," *American Journal of International Law*, Vol. 66, No. 1, 1972.

Casey, Tina, "For Energy Efficiency, US Air Force Aims High in Oklahoma," *Clean Technica*, October 19, 2016. As of September 27, 2018:
https://cleantechnica.com/2016/10/19/
for-energy-efficiency-us-air-force-aims-high-in-oklahoma

Center for Strategic and International Studies, "Significant Cyber Incidents," webpage, undated. As of July 15, 2019:
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

CFR—*See* Council on Foreign Relations.

Copp, Tara, "DoD: At Least 126 Bases Report Water Contaminants Linked to Cancer, Birth Defects," *Military Times*, April 26, 2018. As of September 27, 2018:
https://www.militarytimes.com/news/your-military/2018/04/26/dod-126-bases-report-water-contaminants-harmful-to-infant-development-tied-to-cancers

Council on Foreign Relations, "Cyber Operations Tracker," web tool, undated. As of September 27, 2018:
https://www.cfr.org/interactive/cyber-operations

CSIS—*See* Center for Strategic and International Studies.

Davis, John S. II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-2081-MS, 2017. As of September 21, 2018:
https://www.rand.org/pubs/research_reports/RR2081.html

Deeks, Ashley S., "'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense," *Virginia Journal of International Law*, Vol. 52, No. 3, 2012, pp. 483–550.

Defense Science Board, *Task Force on Cyber Deterrence*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017.

Department of the Air Force, *Electrical Systems, Power Plants and Generators*, Washington, D.C., Air Force Instruction 32-1062, January 15, 2015. As of September 27, 2018:
http://static.e-publishing.af.mil/production/1/af_a4/publication/afi32-1062/afi32-1062.pdf

Department of the Army, *Mineral Exploration and Extraction*, Washington, D.C., Army Regulation 405-30, July 15, 1984.

DoD—*See* U.S. Department of Defense.

Dragos, *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, Hanover, Md., 2017. As of September 27, 2018:
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Droege, Cordula, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," *International Review of the Red Cross*, Vol. 94, No. 886, 2012, pp. 533–578.

Dupree, Jess, "Largest Air Force ESPC Awarded at Tinker ALC," *Energy Express*, January 2017. As of September 27, 2018:
https://www.afcec.af.mil/Portals/17/documents/Energy/Energy%20Express%20JAN_2017.pdf

Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, "Strategic Aspects of Cyberattack, Attribution, and Blame," *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 114, No. 11, 2017, pp. 2825–2830.

Edwards, Paul N., "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems," *Modernity and Technology*, Vol. 1, 2003, pp. 185–226.

Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, Washington, D.C., March 18, 2016. As of October 12, 2018:
https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Executive Office of the President, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, Washington, D.C., August 2013. As of September 27, 2018:
https://www.energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf

Federal Utility Partnership Working Group, "Federal Utility Partnership Working Group Meeting," Williamsburg, Va., November 19–20, 2008. As of August 12, 2019:
https://www1.eere.energy.gov/femp/pdfs/fupwg_fall08_report.pdf

Graham, David E., "Cyber Threats and the Law of War," *Journal of National Security Law and Policy*, Vol. 4, No. 1, 2010, pp. 87–102.

Greenberg, Andy, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017a. As of September 27, 2018:
https://www.wired.com/story/russian-hackers-attack-ukraine

———, "Your Guide to Russia's Infrastructure Hacking Teams," *Wired*, July 12, 2017b. As of October 12, 2018:
https://www.wired.com/story/russian-hacking-teams-infrastructure

Hamre, John J., Deputy Secretary of Defense, "Department of Defense Reform Initiative Directive #9—Privatizing Utility Systems," memorandum to Secretaries of the Military Departments; Chairman of the Joint Chiefs of Staff; Under Secretaries of Defense; Director, Defense Research and Engineering; Assistant Secretaries of Defense; General Counsel of the Department of Defense; Inspector General of the Department of Defense; Director, Operational Test and Evaluation; Assistants to the Secretary of Defense; Director, Administration and Management; Directors of the Defense Agencies; and Directors of the DoD Field Activities, Washington, D.C., December 10, 1997. As of September 27, 2018: http://archive.defense.gov/dodreform/drids/drid9.htm

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review*, Vol. 100, 2012, pp. 817–885.

Hays, Jeffrey, "Scythians," *Facts and Details* blog, May 2016. As of September 27, 2018: http://factsanddetails.com/asian/cat65/sub422/item2700.html

Hines, Paul, Jay Apt, and Sarosh Talukdar, "Trends in the History of Large Blackouts in the United States," *2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century*, Piscataway, N.J.: Institute of Electrical and Electronics Engineers, 2008.

Hirsh, Richard F., *Power Loss: The Origins of Deregulation and Restructuring in the American Electric Utility System*, Cambridge, Mass.: MIT Press, 1999.

Holland, Tom, and Andrew Shore, "Darius, Herodotus and the Scythians," British Museum, webpage, October 27, 2017. As of September 27, 2018: https://blog.britishmuseum.org/darius-herodotus-and-the-scythians

Honeywell, "Honeywell, OG&E Help Modernize Tinker Air Force Base and Save $3.5 Million a Year Through Energy Efficiencies," press release, Oklahoma City, Okla., October 19, 2016. As of September 27, 2018: https://www.honeywell.com/en-us/newsroom/pressreleases/2016/10/honeywell-oge-help-modernize-tinker-air-force-base-and-save-3pt5-million-a-year-through-energy-efficiencies

ICJ—*See* International Court of Justice.

IISS—*See* International Institute for Strategic Studies.

Industrial Control Systems Cyber Emergency Response Team, "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure," webpage, Cybersecurity Infrastructure Security Agency, August 23, 2018. As of September 27, 2018: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

International Committee of the Red Cross, *The Geneva Conventions of 12 August 1949*, Geneva, August 12, 1949.

International Court of Justice, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, The Hague, Netherlands, June 27, 1986.

———, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, The Hague, Netherlands, November 6, 2003.

———, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, The Hague, Netherlands, December 19, 2005.

International Institute for Strategic Studies, "The Armed Conflict Database," webpage, undated. As of July 15, 2019: https://www.iiss.org/publications/armed-conflict-database

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, New York: United Nations, 2001.

Janson, Michael A., and Christopher S. Yoo, "The Wires Go to War: The U.S. Experiment with Government Ownership of the Telephone System During World War I," Penn Law Legal Scholarship Repository, Faculty Scholarship, Paper 467, April 1, 2013.

Jasper, Scott, "Deterring Malicious Behavior in Cyberspace," *Strategic Studies Quarterly*, Vol. 9, No. 1, 2015, pp. 60–85.

Joint Chiefs of Staff, *Joint Bulk Petroleum and Water Doctrine*, Washington, D.C., Joint Publication 4-03, January 11, 2016. As of September 27, 2018: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp4_03pa.pdf?ver=2018-02-08-091424-107

Kattan, Victor, "Israel, Hezbollah and the Conflict in Lebanon: An Act of Aggression or Self-Defense?" *Human Rights Brief*, Vol. 14. No. 1, 2006, pp. 26–30.

Lachman, Beth E., Kimberly Curry Hall, Aimee E. Curtright, and Kimberly Colloton, *Making the Connection: Beneficial Collaboration Between Army Installations and Energy Utility Companies*, Santa Monica, Calif.: RAND Corporation, MG-1126-A, 2011. As of September 27, 2018: https://www.rand.org/pubs/monographs/MG1126.html

Lachman, Beth E., Ellen M. Pint, Gary Cecchine, and Kimberly Colloton, *Developing Headquarters Guidance for Army Installation Sustainability Plans in 2007*, Santa Monica, Calif.: RAND Corporation, MG-837-A, 2009. As of September 27, 2018: https://www.rand.org/pubs/monographs/MG837.html

Lachman, Beth E., Susan A. Resetar, and Frank Camm, *Military Installation Public-to-Public Partnerships: Lessons from Past and Current Experiences*, Santa Monica, Calif.: RAND Corporation, RR-1419-A/AF/NAVY/OSD, 2016. As of September 22, 2018: https://www.rand.org/pubs/research_reports/RR1419.html

Lachman, Beth E., Susan A. Resetar, Nidhi Kalra, Agnes Gereben Schaefer, and Aimee E. Curtright, *Water Management, Partnerships, Rights, and Market Trends: An Overview for Army Installation Managers*, Santa Monica, Calif.: RAND Corporation, RR-933-A, 2016. As of September 21, 2018: https://www.rand.org/pubs/research_reports/RR933.html

Latham, Robert, ed., *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New York: New Press, 2003.

Lewis, Brandon, "Raytheon EMP Weapon Tested by Boeing, USAF Research Lab," *Military Embedded Systems*, undated. As of October 12, 2018: http://mil-embedded.com/news/raytheon-emp-missile-tested-by-boeing-usaf-research-lab/

Li, Sheng, "When Does Internet Disruption Trigger the Right of Armed Self Defense?" *Yale Journal of International Law*, Vol. 38, No. 1, 2013, pp. 179–216.

Luiijf, Eric, Albert Nieuwenhuijs, Marieke Klaver, Michel van Eeten, and Edite Cruz, "Empirical Findings on Critical Infrastructure Dependencies in Europe," in Roberto Setola and Stefan Geretshuber, eds., *Critical Information Infrastructure Security, CRITIS 2008, Lecture Notes in Computer Science*, Berlin, Germany: Springer Link, 2008, pp. 302–310.

Marks, Jay F., "OG&E to Take Over Electrical Operations at Tinker," *The Oklahoman*, October 1, 2010. As of September 27, 2018: https://oklahoman.com/article/3500271/oge-to-take-over-electrical-operations-at-tinker

Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn, *Power Begins at Home: Assured Energy for U.S. Military Bases*, Reston, Va.: Noblis, Inc., 2017.

Marstel-Day, *Army Water Security Strategy*, Fredericksburg, Va., December 2011.

Miller, Erin, *Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970–2015*, College Park, Md.: National Consortium for the Study of Terrorism and Responses to Terrorism, 2016.

Monaco, Lisa, "Expanding Our Ability to Combat Cyber Threats," Washington, D.C.: White House, April 1, 2015. As of October 12, 2018: https://obamawhitehouse.archives.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats

Morrow, J. D., *Game Theory for Political Scientists*, Princeton, N.J.: Princeton University Press, 1994.

Narayanan, Anu, Debra Knopman, James D. Powers, Bryan Boling, Benjamin M. Miller, Patrick Mills, Kristin Van Abel, Katherine Anania, Blake Cignarella, and Connor P. Jackson, *Air Force Installation Energy Assurance: An Assessment Framework*, Santa Monica, Calif.: RAND Corporation, RR-2066-AF, 2017. As of September 21, 2018: https://www.rand.org/pubs/research_reports/RR2066.html

National Institute of Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Gaithersburg, Md., NIST Special Publication 1108, 2010.

———, *Guide to Industrial Control Systems (ICS) Security*, Gaithersburg, Md., NIST Special Publication 800-82 Rev. 2, 2015.

Naylor, Brian, "Russia Hacked U.S. Power Grid—So What Will the Trump Administration Do About It?" NPR, March 23, 2018.

Negroponte, John D., letter from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, S/2001/946, October 7, 2001. As of October 12, 2018: http://www.undocs.org/s/2001/946

Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helga Janicke, "SCADA Security in the Light of Cyber-Warfare," *Computers and Security*, Vol. 31, No. 4, 2012, pp. 418–436.

NIST—*See* National Institute of Standards and Technology.

North American Electric Reliability Corporation, "Standards," webpage, undated. As of July 15, 2019:
https://www.nerc.com/pa/Stand/Pages/Default.aspx

North Carolina Environmental Quality, "NC Water WARN," webpage, 2018. As of September 27, 2018:
https://deq.nc.gov/nc-water-warn

Nye, Joseph S., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4, 2011, pp. 18–38.

Obama, Barack, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," Washington, D.C.: White House, December 29, 2016. As of October 12, 2018:
https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

O'Brien, Brandice J., "Contract Change Enacted Sept. 1; Change Seamless to Team Tinker," Tinker Air Force Base, September 7, 2012. As of September 27, 2018:
https://www.tinker.af.mil/News/Article-Display/Article/385114/contract-change-enacted-sept-1-change-seamless-to-team-tinker/

Office of the Assistant Chief of Staff for Installation Management, "IGSA Partnerships," webpage, undated. As of July 15, 2019:
https://www.acsim.army.mil/partnerships/igsa_partnerships.html

Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, *Department of Defense Annual Energy Management Report Fiscal Year 2015*, Washington, D.C., June 2016. As of September 27, 2018:
https://www.acq.osd.mil/eie/downloads/ie/fy%202015%20aemr.pdf

———, *Department of Defense Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*, Washington, D.C., July 2017. As of September 27, 2018: https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf

Office of the Assistant Secretary of Defense for Legislative Affairs, *Department of Defense Conference Appeals FY15 National Defense Authorization Bill*, Washington, D.C., October 2014. As of September 27, 2018: http://www.taxpayer.net/wp-content/uploads/ported/images/downloads/DoDFY15NDAAAppealstoCongressPackage.pdf

Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections: Intelligence Community Assessment*, Washington, D.C., 2017.

Office of Management and Budget, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs," memorandum for heads of executive departments and establishments, Washington, D.C., October 29, 1992.

Parker, John, "Huge Energy Savings Ahead for Bldg. 9001," Tinker Air Force Base, June 17, 2016. As of September 27, 2018: https://www.tinker.af.mil/News/Article-Display/Article/845292/huge-energy-savings-ahead-for-bldg-9001

Perlroth, Nicole, and David E. Sanger, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," *New York Times*, March 15, 2018.

Perrow, Charles, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*, Princeton, N.J.: Princeton University Press, 2007.

Polityuk, Pavel, "Ukraine to Probe Suspected Russian Cyber Attack on Grid," Reuters, December 31, 2015.

Powell, Robert, *Nuclear Deterrence Theory: The Search for Credibility*, Cambridge, United Kingdom: Cambridge University Press, 1990.

President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Washington, D.C., October 1997. As of September 27, 2018: https://fas.org/sgp/library/pccip.pdf

Public Law 105-85, National Defense Authorization Act for Fiscal Year 1998, November 18, 1997.

Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, June 12, 2002.

Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018.

Quigley, Kevin, "'Man Plans, God Laughs': Canada's National Strategy for Protecting Critical Infrastructure," *Canadian Public Administration*, Vol. 56, No. 1, 2013, pp. 142–164.

Reynolds, Clark G., "Submarine Attacks on the Pacific Coast, 1942," *Pacific Historical Review*, Vol. 33, 1964, pp. 183–193.

Ridley, Gail, "National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience," *Journal of Business Ethics*, Vol. 103, No. 1, 2011, pp. 111–125.

Sanger, David E., "Russian Hackers Appear to Shift Focus to U.S. Power Grid," *New York Times*, July 27, 2018.

Saxton, E. Patrick, "OG&E, Positive Energy Is a Slam Dunk," slide presentation, 2017.

Schaffer, Ronald, "American Military Ethics in World War II: The Bombing of German Civilians," *Journal of American History*, Vol. 67, No. 2, 1980, pp. 318–334.

Schelling, Thomas C., *The Strategy of Conflict*, Cambridge, Mass.: Harvard University Press, 1981.

Schmitt, Michael N., "Cyber Operations and the *Jus ad Bellum* Revisited," *Villanova Law Review*, Vol. 56, No. 3, 2011, pp. 569–606.

———, "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law and Policy Review*, Vol. 25, No. 2, 2014, pp. 269–299.

———, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, United Kingdom: Cambridge University Press, 2017.

Smith, Brad, "The Need for a Digital Geneva Convention," *Microsoft on the Issues* blog, February 14, 2017. As of September 27, 2018: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention

Smith, Chadwick I., "North Korea: The Case for Strategic Entanglement," *Orbis*, Vol. 50, No. 2, 2006, pp. 343–353.

Stockton, Paul, *Electric Infrastructure Protection Handbook II*, Vol. 2: *Water Sector Resilience for Black Sky Events*, Washington, D.C.: Electric Infrastructure Security Council, 2016. As of October 18, 2018: https://www.eiscouncil.org/App_Data/Upload/7f41c325-654e-4c67-be3d-6941645f4485.pdf

Sustainable Ozarks Partnership, "Fort Leonard Wood and Sustainable Ozarks Partnership Accept Army Community Partnership Award," *Phelps County Focus*, December 8, 2017. As of July 15, 2019:
http://www.phelpscountyfocus.com/news/article_f927932e-dc5c-11e7-9655-9f4c63d05161.html

Union of Concerned Scientists, "How the Electricity Grid Works," webpage, February 18, 2015. As of September 27, 2018:
https://www.ucsusa.org/clean-energy/how-electricity-grid-works#.W60ImY0UmUl

United Nations, "UN Charter (Full Text)," San Francisco, June 26, 1945. As of July 15, 2019:
https://www.un.org/en/sections/un-charter/un-charter-full-text/

United Nations Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, New York, A/66/152, July 15, 2011.

U.S. Army Center for Health Promotion and Preventive Medicine, *Emergency Response Planning for Military Water Systems*, Aberdeen Proving Ground, Md., TG-297, 2005.

U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, Washington, D.C., and Ottawa, Canada, April 2004. As of September 27, 2018:
https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf

US-CERT—*See* U.S. Computer Emergency Readiness Team.

U.S. Computer Emergency Readiness Team, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," webpage, Cybersecurity Infrastructure Security Agency, March 16, 2018. As of September 27, 2018:
https://www.us-cert.gov/ncas/alerts/TA18-074A

U.S. Department of Defense, *Department of Defense Guidance for Privatizing Defense Utility Systems*, Washington, D.C., undated. As of July 15, 2019:
https://www.acq.osd.mil/eie/Downloads/IE/guidance.pdf

———, *Mission Assurance Strategy*, Washington, D.C., April 2012a.

———, *Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations*, Washington, D.C., December 19, 2012b.

———, *The DoD Cyber Strategy*, Washington, D.C., April 2015. As of October 12, 2018:
http://archive.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

———, *Economic Analysis for Decision-Making*, Washington, D.C., Department of Defense Instruction 7041.03, October 2, 2017. As of September 27, 2018:
https://fas.org/irp/doddir/dod/i7041_03.pdf

U.S. Department of Defense, Office of General Counsel, *Law of War Manual*, Washington, D.C., December 2016.

U.S. Environmental Protection Agency, "Basic Information About Your Drinking Water," webpage, undated. As of September 27, 2018: https://www.epa.gov/ground-water-and-drinking-water/basic-information-about-your-drinking-water

U.S. Government Accountability Office, *Defense Infrastructure: Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts*, Washington, D.C., GAO-18-558, September 2018.

U.S. Securities and Exchange Commission, "Form 8-K: OGE Energy Corp.," Washington, D.C., December 12, 2005. As of September 27, 2018: https://www.sec.gov/Archives/edgar/data/1021635/000102163505000328/oge8k121505.htm

Verton, Dan, "Software Failure Cited in August Blackout Investigation," *ComputerWorld*, November 20, 2003. As of July 15, 2019: https://www.computerworld.com/article/2573466/software-failure-cited-in-august-blackout-investigation.html

Walker, Neal, "UN Resident Coordinator and Humanitarian Coordinator in Ukraine, Neal Walker: Statement on Humanitarian Impact of Hostilities in Eastern Ukraine," United Nations, November 8, 2017. As of September 27, 2018: https://reliefweb.int/report/ukraine/un-resident-coordinator-and-humanitarian-coordinator-ukraine-neal-walker-statement

Waxman, Matthew, "Cyber Strategy and Policy: International Law Dimensions," testimony before the Senate Armed Service Committee, Washington, D.C., March 2, 2017.

Webster, Andrew, "Hague Conventions (1899, 1907)," in Gordon Martel, ed., *The Encyclopedia of War*, Oxford, United Kingdom: Wiley-Blackwell, November 2011.

Weston Solutions, *Environmental Assessment for Tinker Aerospace Complex Tinker Air Force Base, Oklahoma*, May 2008. As of September 27, 2018: http://www.dtic.mil/dtic/tr/fulltext/u2/a633559.pdf

White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, Washington, D.C., Presidential Policy Directive 21, February 12, 2013.

———, *Report on Cyber Deterrence Policy*, Washington, D.C., 2015. As of October 12, 2018: http://federalnewsnetwork.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

Willingham, William F., "Bonneville Dam's Contribution to the War Effort," *Builders and Fighters*, Vol. 199, 1992, pp. 295–301.

Zetter, Kim, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014.

———, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.

Zhu, Bonnie, Anthony Joseph, and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," *2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, October 2011, pp. 380–388.

About the Authors

Anu Narayanan is an engineer at the RAND Corporation whose research lies at the intersection of critical infrastructure (particularly energy) systems and national security. She has led or conducted studies on this topic for the U.S. Air Force, Department of Energy, Department of Homeland Security, and Office of the Secretary of Defense. Her areas of methodological expertise include probabilistic risk assessment, scenario- and capabilities-based planning, and systems analysis. She holds a Ph.D. in engineering and public policy.

Jonathan William Welburn is an associate operations researcher at the RAND Corporation. His research sits at the intersection of operations research and economics and employs methods from operations research, game theory, computational economics, and analytics. He holds a Ph.D. in decision science and operations research.

Benjamin M. Miller is an economist at the RAND Corporation and a professor at the Pardee RAND Graduate School. He conducts economic assessments that improve public systems, including infrastructure systems, regulatory systems, and financial systems. He holds a Ph.D. in economics.

Sheng Tao Li is a former senior policy analyst at the RAND Corporation, where his research touched on a range of legal topics, from international security to intellectual property. He holds a J.D.

Aaron Clark-Ginsberg is an associate social scientist at the RAND Corporation. His research focuses on natural hazards, community resilience, infrastructure, cybersecurity, and international development. He holds a Ph.D. in humanitarian action.

Increased reliance on intelligence processing, exploitation, and dissemination; networked real-time communications for command and control; and a proliferation of electronic controls and sensors in military vehicles (such as remotely piloted aircraft), equipment, and facilities have greatly increased the U.S. Department of Defense (DoD)'s dependence on energy, particularly electric power, at installations. Thus, ensuring that forces and facilities have access to a reliable supply of electricity is critical for mission assurance. However, most of the electricity consumed by military installations in the continental United States comes from the commercial grid—a system that is largely outside of DoD control and increasingly vulnerable to both natural hazards and deliberate attacks, including cyberattacks. In this report, researchers explore two approaches that DoD might consider as options for deterring attacks against the power grid: enhancing resilience and reliability to deter by denial and using the threat of retaliation to deter by cost imposition. The report represents a first step in developing frameworks and context to support DoD decisionmaking in this area.

$19.50

ISBN-10 1-9774-0416-2
ISBN-13 978-1-9774-0416-9

www.rand.org

RR-3187-RC