SANDIA REPORT
SAND2019-4389
Unlimited Release
Printed Month and Year

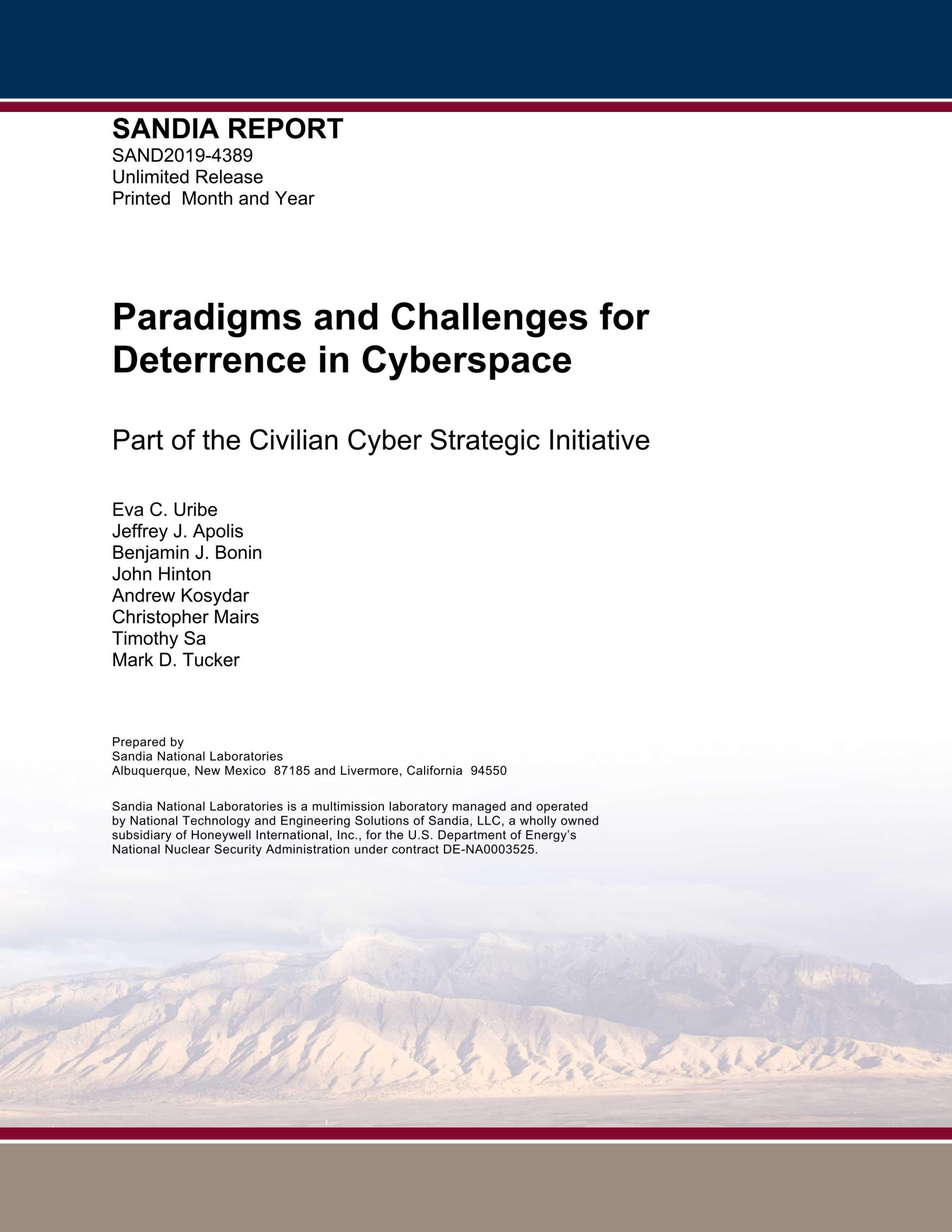
Paradigms and Challenges for Deterrence in Cyberspace

Part of the Civilian Cyber Strategic Initiative

Eva C. Uribe
Jeffrey J. Apolis
Benjamin J. Bonin
John Hinton
Andrew Kosydar
Christopher Mairs
Timothy Sa
Mark D. Tucker

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.




Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

SAND2019-4389
Printed April 2019
Unlimited Release

Paradigms and Challenges for Deterrence in Cyberspace

Part of the Civilian Cyber Strategic Initiative

Eva Uribe
Systems Research & Analysis IV

Jeffrey J. Apolis
Systems Research & Analysis III

Benjamin J. Bonin
Systems Research & Analysis I

John P. Hinton
Special Consultant

Andrew Kosydar
Systems Research & Analysis II

Christopher T. Mairs
Systems Technology

Timothy Sa
Systems Research & Analysis II

Mark D. Tucker
WMD Threats & Aerosol Science

Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MSXXXX

Abstract

In 2018 Sandia National Laboratories launched the Civilian Cyber Strategic Initiative, an ongoing multi-year effort to characterize future threats to civilian cyber infrastructures, to inform research and development efforts to detect, attribute, counter, and recover from cyber attacks, and to inform program and capability investment decisions across the Energy and Homeland Security portfolio at Sandia. One of the primary objectives of the Civilian Cyber Strategic initiative is to leverage Sandia's systems analysis capabilities to characterize future threats and to support a new theory of deterrence. Towards the goal of supporting a new theory of deterrence in cyberspace, the purpose of this study was to understand how new and existing deterrence paradigms can be applied to cyberspace, to identify unique challenges and pitfalls associated with deterring adversaries in cyberspace, and to develop preliminary ideas for how our ability to deter cyber adversaries might be improved. Our approach combined literature reviews of relevant policy documents and the academic literature with interviews of experts both at Sandia and beyond.

ACKNOWLEDGMENTS

The authors would like to thank the Civilian Cybersecurity Strategic Initiative team members and leadership, especially Heidi Ammerlahn and Nerayo Teclemariam for their guidance and support. The authors acknowledge the management team of Division 8000, especially Dori Ellis, for their support of this strategic initiative. The authors also acknowledge significant input from several conversations with experts both inside and outside Sandia, including Michael Bierma (SNL), Ben Bonin (SNL), Christopher Harrison (SNL), Sheryl Hingorani (SNL), John Hinton (special consultant to SNL), Kevin Hulin (SNL), Jarret Lafleur (SNL), Joshua Letchford (SNL), Herb Lin (Stanford University), Jackson Mayo (SNL), Michael Nacht (University of California, Berkeley), Jason Reinhardt (SNL), Max Smeets (Stanford University), and Evan Wolff (Crowell & Moring). Many of their excellent ideas appear in this report.

TABLE OF CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

The purpose of this study was to understand how new and existing deterrence paradigms can be applied to cyberspace, and to identify unique challenges and pitfalls associated with deterring adversaries in cyberspace. During the course of the study, we directed our activities towards answering the following questions:

1. What is the state-of-the-art in cyber deterrence? Which ideas are influencing cyber deterrence policy the most?
2. What are the unique challenges for deterring adversaries in cyberspace?

Our approach to answering these questions included literature reviews of relevant policy documents and the academic literature combined with interviews of experts both at Sandia and beyond.

WHAT IS DETERRENCE?

Deterrence is often conceived as the ability to "prevent from action by fear of consequences," but it can also be defined more broadly as seeking to dissuade an action by influencing a potential adversary's cost/benefit analysis, either by imposing costs or by removing the perceived benefits. We define deterrence as "the creation of conditions that dissuade an adversary from taking unwanted actions, because they perceive that the costs exceed the benefits."

Deterrence of cyber adversaries can occur within domain (threatening to use a cyber response to prevent a cyber attack), or across domains (threatening to use a response from a different domain to prevent a cyber attack). In this study, we include both within domain and cross-domain responses in our concept of deterrence.

Scholars have applied various new and existing paradigms to describe how deterrence may apply in cyberspace. These include:

Deterrence by punishment

Deterrence by punishment occurs when one actor seeks to prevent an adversary from acting by threatening to impose an unacceptable consequence. An effective deterrence threat requires that the threat be communicated to the adversary and credible to the adversary, that the defender must be capable of imposing the consequence, and that the adversary perceives that the costs outweigh the benefits of action, and so refrains from action (Figure 1).

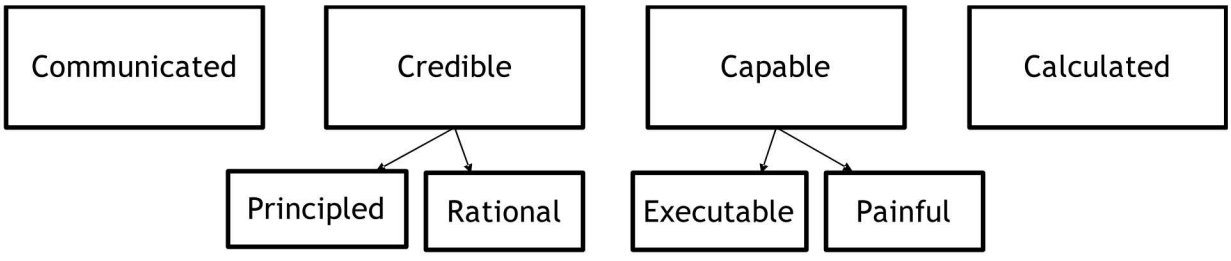


Figure 1. Rational actor theory of deterrence

Deterrence by denial

Deterrence by denial occurs when adversaries are dissuaded from acting because the perceived benefits of their actions have been reduced or eliminated (and therefore denied). There are several ways that deterrence by denial can be strengthened by a deterrer. The deterrer can increase their defenses or the resiliency of their systems, or make attacks more expensive to carry out. The advantage of deterrence by denial measures is that they do not require rapid, high-confidence attribution of attacks.

Deterrence by entanglement

Deterrence by entanglement can be summarized as follows: if you and your adversary are sitting in the same rowboat, you would not attempt to sabotage your adversary by drilling a hole on *their* side of the boat. Deterrence by entanglement can be achieved by fostering "the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim," according to Joseph Nye.

Deterrence by norms

Deterrence by norms describes a situation in which an adversary refrains from actions based on the perception that the damage to his or her reputation will outweigh the perceived benefits of the action.

Cumulative deterrence, punctuated deterrence, and cyber persistence

Cumulative deterrence is achieved using threats combined with actual use of force to gain smaller victories throughout an extended conflict. Through regular use of force, the deterrer establishes "rules of the game" or norms that over time reduce their adversary's incentives for conflict. Punctuated deterrence is a similar concept in which the deterrer applies threats and the actual use of force on an irregular (or punctuated) basis.

Michael Fischerkeller and Richard Harknett argue that for cyber attacks below the threshold of armed attack, deterrence concepts do not apply because deterrence has already failed. Their concept of cyber persistence is similar to cumulative and punctuated deterrence, but focuses less on deterring and more on actively engaging with adversaries. Cyber persistence is "a strategy based on the use of cyber operations, activities and actions (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in cyberspace."

In his seminal paper "Deterrence and Dissuasion in Cyberspace," Joseph Nye argues that no single mechanism for deterrence will succeed in dissuading all actors or preventing all attacks. However, they can work in concert to deter more attacks than deterrence by punishment alone. His table summarizing which actors and what behaviors are most deterred by which types of deterrence is shown below:

The How, Who, and What of Cyber Deterrence and Dissuasion

How	Punishment	Denial/Defense	Entanglement	Norms/Taboos
Who	Both state and	Small states and	Major states such	Major states; less so

	non-state actors	nonstates, but not advanced persistent threats	as China; less so North Korea	rogues; some nonstates
What	Major use of force; sanctions against sub-LOAC* levels of activity	Some crime and hacking; imperfect against advanced states	Major use of force; major sub-LOAC actions	LOAC if use of force; taboo on use against civilians; norms against cybercrime

*LOAC stands for Law of Armed Conflict

HOW CAN WE DETER CYBER ADVERSARIES – AN EVOLVING DEBATE

Past and current U.S. deterrence policy for cyberspace

Similar to scholars of deterrence theory, policy makers are still grappling with whether and how deterrence should be included in a comprehensive U.S. strategy to advance U.S. interests and prevent conflict and escalation in and through cyberspace. The full report includes a description of past and current deterrence policy for cyberspace. Key highlights include:

- A Trump administration report on the nation's strategic options for deterring adversaries in cyberspace distinguishes between attacks that constitute a use of force and those below the threshold for the use of force: "The United States remains in a strong position to deter attacks that would constitute a use of force because traditional tools of deterrence remain effective and potent…However, there are significant challenges in deterring the substantial increase in malicious state-sponsored cyber activity occurring below the threshold of the use of force."
- On May 4, 2018, U.S. Cyber Command was elevated to a Unified Combatant Command. It's new Command Vision states that adversaries are operating below the threshold of armed conflict to "weaken our institutions and gain strategic advantages." As a solution, it proposes increased resiliency, defending forward, and cyber persistence to contest malicious cyber actors.

International law and the problem of thresholds

The question of how to discuss and define thresholds is one that the Civilian Cyber Strategic Initiative grappled with throughout the year, and we believe further discussion is merited here at the laboratory and by policymakers at the national level.

There are good reasons for dividing operations into those that are above the threshold of armed conflict and those that are below. There are already well-established international norms defining what constitutes "armed attacks" or "acts of war" that trigger the relevance of the Law of Armed Conflict. How do we know when a cyber attack reaches the level of armed attack? If a cyber attack results in one death, does this constitute armed attack? Are cyber attacks perceived inherently different than "kinetic" attacks that have the same physical effects? Even if we can agree on a threshold, strategic attacks are occurring below the threshold of armed attack. How does international law apply to these conflicts

The role of uncertainty in deterring cyber adversaries

To what extend should thresholds for our response to cyber attacks be clear versus ambiguous? Throughout the history of the Cold War, various schools of thought developed on the role of uncertainty and strategic ambiguity in effective deterrence. The inherent characteristics of the cyber domain pose new questions to this old debate.

Thresholds may increase deterrence effectiveness

We argue that consideration of thresholds increases deterrence effectiveness because it helps define *who* is being deterred and by which mechanisms. Cyber attacks occur across the spectrum of severity. Some are potentially so severe that we would want to deter all of them. Others are less catastrophic and are more analogous to crime: we want to deter some, but acknowledge we can never deter all. Figure 2 shows these notional thresholds.

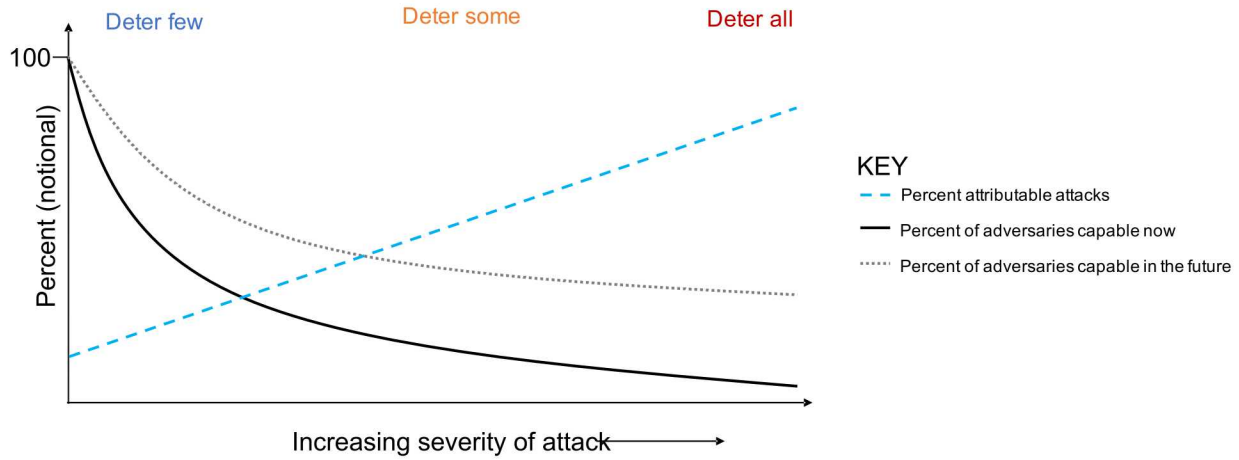


Figure 2. Notional categories for crafting deterrence policy goals

There is general consensus that as the severity of attacks increase, the number of capable adversaries decreases. The precise shape of this correlation is not known, and it is constantly evolving. However, if this trend is true, then it means that as attacks become more severe, they also become easier to attribute. Deterrence by punishment may then play a prominent role at the highest end of the severity scale, where other mechanisms (entanglement, norms, and denial) may also be effective. At lower levels of severity, there are far more actors. Attribution becomes more difficult, and deterrence by punishment plays little to no role. Denial, entanglement, and norms mechanisms may dominate here, as well as concepts of cumulative or punctuated deterrence and cyber persistence.

UNIQUE CHALLENGES OF DETERRENCE IN CYBERSPACE

Cyberspace is different than other physical domains (land, air, sea, space) in many ways, and these characteristics present a number of challenges for deterrence.

Inherent domain characteristics – Cyberspace is a domain of *constant contact*, meaning that a very large number of actors can operate with very low-cost barriers, to produce effects that are

not constrained by special boundaries or time. The Internet allows us all to be connected to everyone else all of the time.

Attack detection – Cyber attacks and exploits are difficult to detect. If the deterrer does not know for weeks or months that an attack has occurred, their response or retaliation will be delayed in time, potentially indefinitely.

Attack attribution – A cyber attacker may easily conceal his or her identity, making rapid, high-confidence attribution very difficult (or impossible). Furthermore, attribution is far more complex than simply answering the question *Who did it?* In this case, *who* can refer to a machine, its owner, its operator, or its location. Stipulating all of these does not answer the question of *who* in fact is responsible. Attribution of a malicious cyber incident also requires asking *Did the adversary intend these effects?* and *Can attribution be proved to others?*

Escalation control across domains – Deterrence of cyber adversaries is inherently a cross-domain deterrence challenge. Schelling has argued that deterrence is more likely to succeed if the response matches the initial attack. Expanding the conflict into other domains may increase changes of escalation.

Asymmetric vulnerability – In cyberspace, the United States is more vulnerable than most (or all) of its potential adversaries, because it relies more on digital systems for daily operation of society and government, and because it possesses more of these systems. This asymmetric vulnerability would logically make any defender wary starting, sustaining, or escalating any conflict in cyberspace, which can impede credible responses to threats and attacks.

Lack of international norms and laws – Compared to the physical domains, where conflict norms are driven by the concepts of state sovereignty and territorial integrity, cyberspace has very few norms, in part because it is a new domain and in part because it lacks territorial boundaries.

Lack of domestic laws and private sector regulation – Cyber systems support almost every aspect of our government, military, and private sectors. Decision-making about detecting, attributing, and responding to attacks is highly decentralized. Who do adversaries perceive is responsible for creating deterrence policies (whether they are deterrence by punishment or deterrence by denial)?

Uncertain effects of cyber weapons – The effects of some cyber operations may be hard to control, while others may be highly precise in their effects. A victim of a cyber attack therefore will not necessarily know whether their adversary intended to produce the effects that occurred, or whether it was a mistake. This makes development of proportional responses difficult.

Blurred lines between offense and defense –The constant contact nature of cyberspace means that offense might begin in my own network, while defensive operations may begin in the networks of others. What one actor might perceive as defensive reconnaissance to prevent or anticipate attacks, another actor might perceive as preparing the battlefield for a future attack.

NOMENCLATURE

Abbreviation	Definition
CCSI	Civilian Cyber Strategic Initiative
CNA	computer network attack
CNE	computer network exploitation
DSB	Defense Science Board
FFRDC	Federally Funded Research and Development Center
LOAC	Law of Armed Conflict
NC3	Nuclear command, control and communications
NPR	Nuclear Posture Review
PEO	Presidential Executive Order
PLC	programmable logic controller
SME	subject matter expert
UNGGE	United Nations Group of Governmental Experts

1. INTRODUCTION

Resilient and secure global civilian information technology and control systems infrastructures are foundational to United States (U.S.) economic and political health, as well as projecting non-military influence abroad. Adversaries, including nation state competitors, non-state actors, and criminal organizations have access to increasingly sophisticated technical capabilities which can disrupt or manipulate those infrastructures.

Towards the goal of supporting a new theory of deterrence in cyberspace, the purpose of this study was to understand how new and existing deterrence paradigms can be applied to cyberspace, and to identify unique challenges and pitfalls associated with deterring adversaries in cyberspace. During the course of the study, we directed our activities towards answering the following questions:

1. What is the state-of-the-art in cyber deterrence? Which ideas are influencing cyber deterrence policy the most?
2. What are the unique challenges for deterring adversaries in cyberspace?

Our approach to answering these questions included literature reviews of relevant policy documents and the academic literature combined with interviews of experts both at Sandia and beyond.

This report is organized in three parts. In the first part, we examine various definitions of deterrence, including deterrence by punishment, by denial, by entanglement, and by norms. In the second part, we investigate questions central to how to deter cyber adversaries, including a review of past and current U.S. policy, and discussions on international law, the problem of establishing response thresholds, and the role of uncertainty in deterrence. In the third part, we have compiled a list of unique challenges for deterring adversaries in cyber space, including the low cost to entry that results in a multitude of actors, a lack of territorial boundaries, slow attack detection, the difficulty of attack attribution, the difficulty of controlling escalation across domains, the asymmetric vulnerability of the United States to attack, a lack of international norms and laws in cyberspace, a lack of domestic laws and regulatory frameworks, the uncertain effects of cyber weapons, and the difficulty of distinguishing between offense and defense in cyberspace.

2. WHAT IS DETERRENCE?

2.1. Exploring multiple concepts of deterrence

Thomas Schelling defined deterrence as the ability to "prevent from action by fear of consequences,"[1] which has been adapted by the Department of Homeland Security Risk Lexicon as "a measure that discourages an action or prevents an occurrence by instilling fear, doubt, or anxiety." Defending against the possibility of a large-scale nuclear attack proved very difficult during the Cold War, so naturally deterrence theory focused on deterrence by threat of punishment or consequence. However, other conceptions of deterrence include defense or other methods to deny the perceived benefits of action to the adversary. In 2017 the Defense Science Board Taskforce on Cyber Deterrence defined *deterrence* as "the use of both deterrence by denial and deterrence by cost imposition to convince adversaries not to conduct cyber attacks or costly cyber intrusions against the United States."[2] Similarly, Kaufmann argues, "deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability actually to achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him."[3]

Therefore, in a more general sense, deterrence can be conceived as influencing the cost/benefit analysis of a potential attacker in order to make the perceived gains less than the perceived costs of action. Snyder describes deterrence as follows: "Deterrence is a function of the total cost-gain expectations of the party to be deterred, and these may be affected by factors other than the apparent capability and intention of the deterrer to apply punishments or confer rewards." For example, he argues, an aggressor may be prevented from action by his or her own conscience, or by perceived damage to his or her reputation. For this study, we adopt the broader concept of deterrence as the attempt to influence an adversary's cost/benefit calculus. Deterrence involves creating conditions that dissuade an adversary from taking unwanted actions, because they perceive that the costs exceed the benefits.

2.2. Deterrence within domains and across domains

The phrase *cyber deterrence* is ambiguous – it is not clear if cyber weapons are being used to deter unwanted behavior or if attacks on cyber assets are being protected using a range of other deterrence tools and techniques. The Civilian Cyber Strategic Initiative is broadly concerned with protecting our civilian critical infrastructure from cyber attack. Therefore, we prefer the phrase *deterrence of cyber adversaries* to clarify that we seek ways to deter potential cyber attacks.

Deterrence of cyber adversaries can occur within domain (threatening to use a cyber response to prevent a cyber attack), or across domains (threatening to use a response from a different domain to prevent a cyber attack). In this study, we include both within domain and cross-domain responses in our concept of deterrence. Deterrence of cyber adversaries therefore exists as a sub-category of cross-domain deterrence,[4] which itself falls under the more encompassing concept of *tailored deterrence*.[5]

The increasing dependence on cyber systems of the U.S. military, including conventional warfighting capabilities and our nuclear command, control, and communication (NC3) systems, means that cybersecurity may impact our strategic stability with other states. For example, if a

state were to attempt a cyber attack that would inhibit another state's ability to control their own nuclear arsenal, a situation could arise in which one state is incentivized to strike first. Clearly, we would want to deter this type of attack. Cyber has an impact on the deterrence relationships between nations.

This impact is extremely important to consider, and has been considered elsewhere.[6] For example, one of the recommendations of the Defense Science Board Taskforce on Cyber Deterrence is for U.S. Strategic Command to conduct "an annual assessment of the cyber resilience of the U.S. nuclear deterrent" including NC3, platforms, delivery systems, and warheads.[2] Similarly, the 2018 Nuclear Posture Review announced a series of initiatives to ensure that our NC3 systems remains "survivable and effective," including an initiative to strengthen protection against cyber threats.[7] However, we consider the challenge of securing nuclear systems from cyber attack to be central to the discussion of nuclear deterrence, which lies primarily within the military realm. The focus of this study is on deterring adversaries from attacking civilian cyber systems, and so the very important question of how to deter adversaries from disrupting strategic stability in the nuclear domain is not discussed further in this report.

2.3. Types of deterrence

The most contemporary and comprehensive discussion of deterrence theory applied in cyberspace can be found in "Deterrence and Dissuasion in Cyberspace" by Joseph S. Nye Jr.[8] In his article, Nye discusses four deterrence mechanisms that apply in cyberspace: deterrence by punishment, deterrence by denial, deterrence by entanglement, and deterrence by norms. Each of these will be discussed further below.

2.3.1. Deterrence by punishment

Deterrence by punishment is the classical notion of deterrence, in which one actor seeks to prevent an adversary from acting by threatening to impose an unacceptable consequence. Deterrence by punishment may seem simple in theory, but in practice it is vastly complex, as it relies on the subjective perception of the actor being deterred, not on the objective intention or capability of the deterrer. Deterrence is in the mind of the actor being deterred. During the Cold War, the rational actor model dominated deterrence theory. We define a rational actor as someone who makes an effort to conduct a reproducible cost/benefit analysis in order to make a decision.

There are plenty of problems with viewing deterrence through the rational actor lens. For example, nation-states and governments are complex, bureaucratic organizations that are made up of people with conflicting and often competing perspectives, goals, and motives. It is not clear that reducing these complex organizational dynamics to a single rational actor is valid. Additionally, countless studies have shown that even individuals do not predictably behave rationally. Nonetheless, it can be argued that failures of deterrence are not the result of failures in the rational actor model, but rather failure on the part of the deterrer to fully understand the type of cost/benefit analysis that their adversary would conduct. Tor deconstructs 'strategic rationality' into 'instrumental rationality' and 'normative rationality.' The former is a strict, mathematical cost/benefit analysis and is indifferent to the actors involved, while the second is "the cost-benefit considerations derived from the value an actor assigns to the elements of the cost-benefit equation; this value is relative and not absolute, and changes from actor to actor."[9] In other words, rationality is in the eye of the beholder.

According to rational actor theory, in order for a deterrence threat to succeed in preventing unwanted action by an adversary, four requirements must be met (Figure 1).[10] If any one of these four requirements fail, deterrence will also fail. These are:

1) **Communicated** – The deterrer's counter threat must be communicated to the adversary, and the adversary must receive and comprehend this communication in the way that the deterrer intended.

2) **Credible** – The deterrer's counter threat must be perceived as credible by the adversary. Credibility requires that the adversary perceive the deterrer's threat as principled, that is, consistent with the deterrer's true and stated value system and conforming to the deterrer's understanding of proportionality. Credibility also requires that the adversary perceive the deterrer's threat as rational, or based on a cost/benefit analysis to achieve the best interests of the deterrer.

3) **Capable** – The adversary must perceive the deterrer as being capable of carrying out their threat. They must believe that the deterrer has the ability to execute the stated threat, and they must view that threat as sufficiently painful enough to outweigh the perceived benefits of their actions.

4) **Calculated** – The adversary must conduct a calculation of the costs and benefits of action, which includes consideration of the threat made by the deterrer, and choose to act in their own best interest.

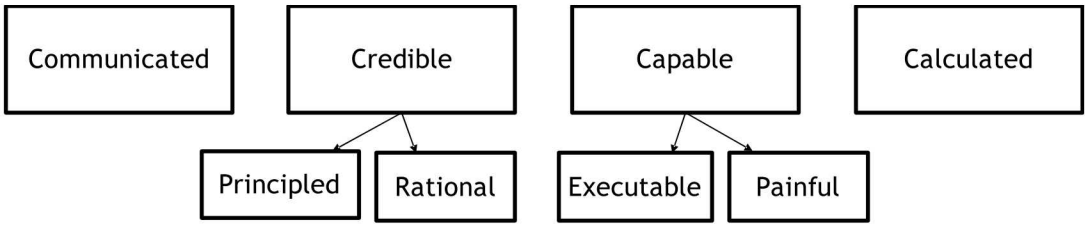


Figure 1. Rational actor theory of deterrence[10]

There are two different types of deterrence by punishment relationships that can be established between two parties. The first is a *preponderance of power* deterrence relationship, in which one party has a clear superior capability such that it is not in the best interests of the second party to conduct unwanted actions. The second is a relationship of *mutual vulnerability* in which both parties have strong capabilities, such that it is in the interests of neither party to initiate conflict. In considering the establishment of stable deterrence relationships in cyberspace, it is important to consider which type of relationship the United States wishes to establish with which actors.

In the literature, we have sometimes seen the phrase *deterrence by cost imposition* used interchangeably with *deterrence by punishment*, because retaliation may be considered a cost that the adversary must bear if they take the action that the deterrer is trying to prevent. However, deterrence by cost imposition can also mean that the deterrer takes measures to literally increase the cost of an attack – to make the attack more expensive to carry out in terms

of resources or time required. This concept of deterrence more properly fits under the second deterrence mechanism, deterrence by denial.

2.3.2. Deterrence by denial

Deterrence by denial occurs when adversaries are dissuaded from acting because the perceived benefits of their actions have been reduced or eliminated (and therefore denied). There are several ways that deterrence by denial can be strengthened by a deterrer. First, the deterrer can increase their defenses. Increased defenses make it more difficult for adversaries to conduct successful cyber intrusions or cyber attacks. Initially, this might not deter attacks that are already underway. Yet as adversaries learn that their attacks are failing more often, and that they must invest more time and resources to ensure that their attacks succeed, they may be deterred from attacking in the first place.

System resiliency also contributes to deterrence by denial. If an adversary observes that the desired effects of their attacks are denied because the target can easily recover from or compensate for damage, then they may refrain from conducting similar types attacks or from attacking similar targets in the future.

As discussed above, deterrence by cost imposition, in which a deterrer seeks to make attacks on their cyber systems more expensive, may also be considered deterrence by denial. Stronger defensive measures increase the cost of attacks. Additionally, increasing the heterogeneity and complexity of systems also makes them costlier to attack. While increasing the heterogeneity of systems also makes them harder to defend, experts generally agree that this decrease in defensibility is compensated for by the difficulty in attacking multiple critical systems at once. If all of your cyber systems are different, then it is more difficult for any one attack to disable several or all of them.

The advantage of deterrence by denial measures is that they do not depend on who is carrying out the attack. High-confidence attribution of attacks is not necessary. Prompt detection of attacks is necessary only to the degree that additional defense and resiliency systems need to be developed and implemented. Efforts to increase defense, heterogeneity, complexity, and resiliency also serve to protect systems from non-malicious cyber events, such as system malfunctions, human errors, natural disasters, and solar storms.

2.3.3. Deterrence by entanglement

Nye defines deterrence by entanglement as “the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim.”[8] Stated another way, an adversary may be deterred from taking an action if the action disrupts a status quo that benefits both the target and the adversary. Deterrence by entanglement can be summarized as follows: if you and your adversary are sitting in the same rowboat, you would not attempt to sabotage your adversary by drilling a hole on *their* side of the boat.

The advantage of deterrence by entanglement is that it does not rely on retaliatory threats, and is thus indifferent to prompt attribution. It also does not require robust defenses or highly resilient systems. However, not all actors are entangled with each other. Rogue, isolated nation-states that have few ties with the outside world will not be as dissuaded by entanglement than nations that are highly connected to the international world order. Another disadvantage is that entanglement may be hard to observe, quantify, and credibly signal. Entanglement and interdependencies often

do not reveal themselves until an action has been taken and the adversary feels the negative effects of their miscalculation.

2.3.4. Deterrence by norms

Deterrence by norms describes a situation in which an adversary refrains from actions based on the perception that the damage to his or her reputation will outweigh the perceived benefits of the action. Norms develop over time and with shared experiences, and in the cyber realm, we are in the very earliest stages of developing norms and codes of conduct.[8] For example, in the nuclear domain, the Nonproliferation Treaty has helped perpetuate the norm against the development of nuclear weapons by states that do not already possess them. The non-use of nuclear weapons in all conflicts since WWII has resulted in an international norm against exploding nuclear weapons in combat. The Biological Weapons Convention and the Chemical Weapons Convention have helped to solidify norms against possession and use of biological and chemical weapons.

Establishing norms against cyber attacks may be possible, but presents additional challenges. Computer code is notoriously dual-use: the same programs can be used for innocuous and malicious activity. Therefore, as Nye observes, it is unlikely that norms will progress through the prohibition of entire classes of cyber tools. Norms are more likely to progress through anathematizing classes of targets, such as certain critical civilian targets during peacetime. So far, this has been the approach of the United States and the United Nations Groups of Governmental Experts (UNGGE).

2.4. Additional challenges

Deterrence by punishment was the predominant, although not the primary, basis for nuclear deterrence during the Cold War. Significant efforts were made to contribute to the adversary's perspective that the general population of the U.S. could withstand and recover from nuclear war. Air defenses were erected. Fallout shelters were built. School children practiced "duck and cover" drills. However, most regarded the possibility of defending against a large-scale nuclear attack as remote. The nuclear domain is generally viewed as dominated by offense, not defense.

The same cannot be said for the cyber domain, in which the perception of strong defense and resiliency is more realistic, and the Internet serves to entangle the politics and economies of the world. One of Nye's central arguments is that deterrence by denial, entanglement, and norms will play a larger role for cyberspace than they did for the nuclear domain, and that deterrence by punishment will play a relatively smaller role. Sole reliance on deterrence by punishment "may miss some of the most important political behavior that indicates that deterrence and dissuasion are working in the cyber realm despite the problem of attribution," according to Nye.[8]

The advantage of deterrence by denial, entanglement, normative means is that these do not rely on prompt, high-confidence attack detection and attribution in the same way that deterrence by punishment does, and they are potentially effective against a wider range of actors. However, there are still significant challenges. Each of these concepts still relies on communication or shared understanding between the attacker and the defender. As Nye observes, "Had Japan better understood the resilience of the United States after Pearl Harbor, it might have made a more accurate calculation about the costs and benefits of the attack."[8] Merely possessing resilient systems does not constitute effective deterrence. U.S. resiliency to attack before Pearl Harbor did not prevent the attack on Pearl Harbor. Resiliency can increase the likelihood of deterrence over

time, as adversaries learn that the effectiveness of their attacks is diminished by our ability to adapt and recover. However, resiliency, unless it is properly communicated, does not have a chance at deterring every attack every time.

The same can be argued for deterrence by entanglement and deterrence through norms. Entanglement may be also hard to signal. Can we enact policies or make declaratory statements that increase the likelihood that we and our potential adversaries have a common understanding of our entanglement? Moreover, we may not be entangled with every adversary that we wish to deter. However, one advantage to deterrence by entanglement is that in the modern era, where information is shared at unprecedented rates, it may be easier for states to discern and communicate their entanglement than it was before the advent of the cyber era.

2.5. Who and what can be deterred – and how?

Nye's central argument is that whether or not deterrence theory can be properly applied in cyberspace depends on who is being deterred, what actions are being deterred, and how they are being deterred. A summary of which actors and what behaviors are most easily deterred by punishment, denial, entanglement, and norms is provided in Table 1, which is reproduced exactly from Nye's article.

Table 1. The How, Who, and What of Cyber Deterrence and Dissuasion[8]

How	Punishment	Denial/Defense	Entanglement	Norms/Taboos
Who	Both state and non-state actors	Small states and nonstates, but not advanced persistent threats	Major states such as China; less so North Korea	Major states; less so rogues; some nonstates
What	Major use of force; sanctions against sub-LOAC* levels of activity	Some crime and hacking; imperfect against advanced states	Major use of force; major sub-LOAC actions	LOAC if use of force; taboo on use against civilians; norms against cybercrime

*LOAC stands for Law of Armed Conflict

The major implication of Nye's work is that no single mechanism of the four discussed (punishment, denial, entanglement, or norms) can deter all types of cyber attacks. However, together they may work in concert to prevent more types of attacks than would deterrence by punishment alone.

2.6. Cumulative Deterrence, Punctuated Deterrence, and Cyber Persistence

Two additional concepts of deterrence have recently surfaced in the literature, *cumulative* deterrence and *punctuated* deterrence. In his exposition on cumulative deterrence,[9] Tor distinguishes *absolute* deterrence from *restrictive* deterrence. Absolute deterrence is when one party wishes to deter all acts of violence of a specific type from their adversary. Absolute deterrence is the bedrock of the nuclear deterrence relationships between large nuclear-armed nation states. In contrast, restrictive deterrence is when one party seeks to influence conflict to minimize the impact of violence, while realizing that total prevention is impossible. He contrasts deterrence theory developed in the U.S. during the Cold War with deterrence theory developed in Israel throughout its history contending with ground invasion by neighboring states and facing continual attacks on civilian populations by non-state actors: "The U.S. focused on the questions

of how to maximize its benefit from nuclear weapons without ever using them…Israel, on the other hand, was preoccupied with the dilemma of how to postpone, limit, and shape a series of ongoing conflicts with a variety of state and sub-state actors."[9]

Cumulative deterrence is restrictive in nature and seeks to convince adversaries over time that conflict will not serve their purpose. This is achieved using threats and actual force to gain smaller victories during an extended conflict. Tor describes the concept as follows: "On the macro level, it seeks to create an image of overwhelming military supremacy, while on the micro level it relies on specific military responses to specific threats or hostile acts. According to this concept, deterrence needs to be 'recharged' from time to time through a series of victories accumulated over extended periods throughout the conflict, which produce a more moderate behavior on the part of the adversary."[9] Through regular use of force, the deterrer establishes "rules of the game" or norms that over time reduce their adversary's incentives for conflict.

Tor proposes that this concept of deterrence is more relevant for conflict in cyberspace than absolute deterrence concepts borrowed from the nuclear domain. A strategy of cumulative deterrence in cyberspace would be comprised of the following elements, according to Tor:

1. A clear strategic message communicating the thresholds of the deterring party
2. The ability and willingness to use force against rivals on a consistent basis, through cyber, kinetic, diplomatic, or financial means to demonstrate resolve
3. The ability and willingness to demonstrate capabilities of cyber, kinetic, diplomatic, and financial tools
4. Overwhelming supremacy in cyberspace
5. Investment in a more robust and secure cyber infrastructure to make attacks more difficult and more costly

Kello's related concept of *punctuated* deterrence "prescribes a response to a series of actions and cumulative effects, rather than individual actions and particular effects."[11] The major distinction is that while cumulative deterrence would involve consistent use of force in response to precipitating events, punctuated deterrence calls for a less exhaustive approach that capitalizes on the effects of uncertainty in the mind of the deterred: "not continuous reprisals…but a graduated scheme in which penalties are meted out over time and at a moment of the defender's choosing."[11]

These two concepts of deterrence are part of an increasing trend in the academic literature that emphasizes the role of persistent, offensive retaliatory measures in establishing norms, pursuing interests, and preventing conflict in cyberspace.

Fischerkeller and Harknett go so far as to say that deterrence is not a credible strategy for dissuading cyber adversaries at all, due to the inherent nature of interaction between actors in cyberspace.[12] Deterrence "is a strategy based upon a threat of use of force with an operational objective of avoiding costly operational contact (i.e., the actual use of force."[12] They argue that deterrence is the tool of those who want to avoid fighting wars, not of those who want to fight and win wars that are already happening. As Bernard Brodie wrote in 1946 at the dawn of the

atomic age, “Thus far, the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose.”[13] While the primary purpose of a strategy of deterrence is to avoid operational contact, cyberspace is “a perpetually contested space,” in which a multitude of actors are in operational contact right now, and all the time. Therefore, a strategy of deterrence is not suited to achieving one’s objectives in cyberspace.

Instead, they propose a strategy of cyber *persistence*. Cyber persistence is “a strategy based upon the use of cyber operations, activities and actions (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in cyberspace so that the United States could ultimately deliver direct effects in, through, and from cyberspace at a time and place of its choosing.”[12] Fischerkeller and Harknett argue that deterrence, based on restraint, restricts behavior of the U.S. and other “like-minded” states in cyberspace. Through persistent operations, activities, and operations, these states can have a stronger role in shaping the norms of cyber conflict that are already being developed by others: “Global cyberspace norms of responsible behavior cannot take root if the universe of ‘like-minded’ states is a small proportion of salient cyber actors.”[12]

It is important to note that the authors of the concepts of cumulative deterrence, punctuated deterrence, and cyber persistence described above consider *deterrence* in the narrower concept of *deterrence by punishment*. Nonetheless, their views have become increasingly relevant to U.S. policymakers, as will be described in the next section.

3. HOW CAN WE DETER CYBER ADVERSARIES? – AN EVOLVING DEBATE

Similar to scholars of deterrence theory, policy makers are still grappling with whether and how deterrence should be included in a comprehensive U.S. strategy to advance U.S. interests and prevent conflict and escalation in and through cyberspace. Below we summarize the evolution of U.S. policy for deterrence of cyber adversaries. These summaries are followed by discussion of two attributes of deterrence that are still heavily debated: the problem of establishing and communicating response thresholds, and the role of uncertainty in cyberspace. We argue that a discussion of response thresholds is critical for developing effective deterrence policies because it helps to define precisely who and what we wish to deter.

3.1. Past U.S. policy for deterrence in cyberspace

Schneider provides an excellent history of U.S. policy for deterring cyber adversaries through 2016.[14] Serious consideration of developing a policy of deterrence for cyberspace began in the Obama administration in 2009. At the time, it was recognized that the difficulty of attributing cyber attacks challenged traditional, retaliatory deterrence by punishment in many cases.[15] The administration's initial Comprehensive National Cybersecurity Initiative therefore included an initiative to develop "a defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors."[16]

Prior to 2009, the U.S. military cyber defense effort was shared by a number of separate task forces within the military. Defense Secretary Gates collected the disparate task forces into a one combatant command within Strategic Command in 2010. President Obama's 2011 International Strategy for Cyberspace included a section entitled "Defense: Dissuading and Deterring," which outlined an approach that would combine resilience with response: "We will seek to encourage good actors and dissuade and deter those who threaten peace and stability…We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options."[17]

There are competing views about the effectiveness of cyber deterrence efforts in the years between 2011 and 2015. Nye describes a series of attacks that could all be considered "failures of deterrence," but all were considered low-threshold attacks with limited impact on national security.[8] Schneider describes a series of responses the U.S. made to cyber events that strengthened its credibility for deterrence by punishment,[14] including Executive Order 13694, which allowed the Treasury Department to enact sanctions to respond to cyber attacks. During this time, the State Department released recommendations for norms in cyberspace, and Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience" designated sixteen U.S. critical infrastructure sectors,[18] to signal to potential adversaries that the U.S. wanted to deter attacks against these specific civilian targets. Despite these efforts, the Obama administration was criticized of not having a coherent deterrence strategy, partly based on its emphasis on defense and deterrence by denial instead of deterrence by punishment.[8]

The 2015 Department of Defense Cyber Strategy increased its focus on deterrence and explicitly includes the concept of deterrence by punishment (or deterrence by *response*) in a broader definition that also encompasses denial: "Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an

attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed."[19] They propose three areas that contribute to deterrence, including response, denial, and resilience, as well as efforts to reduce anonymity of state and non-state actor activity in cyberspace to advance attribution. The 2015 strategy further states that in conducting all cyber operations, the U.S. will follow a "doctrine of restraint" in accordance with the Law of Armed Conflict.

3.2. Current and evolving U.S. policy for deterrence in cyberspace

The 2017 National Security Strategy recognizes the central role that cyberspace plays in advancing U.S. interests and national security objectives. The National Security Strategy describes three challenges and opportunities related to cybersecurity: 1) that threats in cyberspace may be tantamount to strategic threats, 2) that we must be able to deter both by imposing "swift and costly consequences" and by building more resilient critical infrastructure, and 3) that attribution is difficult, and in some cases impossible.[20] The strategy further requires that the Department of Defense "develop new operation concepts and capabilities to *win without assured dominance* in air, maritime, land, space, and cyberspace domains, including against those operating below the level of military conflict."[20]

One of the Trump administration's early Presidential Executive Order (PEO) 13800 "On Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" required his administration to assess "the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats."[21] The unclassified summary report issued one year later called on the U.S. and its partners to "deter destabilizing state conduct in cyberspace."[22]

This report distinguishes between two types of attacks: those that constitute a use of force and those that occur below the threshold of the use of force: "The United States remains in a strong position to deter attacks that would constitute a use of force because traditional tools of deterrence remain effective and potent…However, there are significant challenges in deterring the substantial increase in malicious state-sponsored cyber activity occurring below the threshold of the use of force." For cyber attacks below the threshold of the use of force, the authors of the report recommend "deterrence by denial through defense and protection of critical infrastructure…and timely recovery from malicious cyber activities." The report defines two goals of deterrence moving forward:

1. A continued absence of cyber attacks that constitute a use of force against the U.S., partners, and allies
2. Reduction in destructive, disruptive, or destabilizing cyber activities against U.S. interests below the threshold of the use of force

On May 4, 2018, U.S. Cyber Command, which was previously under the auspices of Strategic Command, was elevated to a Unified Combatant Command. In March, Cyber Command issued its new Command Vision, "Achieve and Maintain Cyberspace Superiority."[23] Similarly to the National Security Strategy and the report in response to PEO 13800, the Vision distinguishes between attacks above and below the threshold of the use of force. But the Vision goes a step further: "Adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages."[23] Not only are adversaries operating below the

threshold of armed conflict, where deterrence is most difficult, but they are having strategic effects. Therefore, the second goal established in report in response to PEO 13800, to *reduce* destructive, disruptive, or destabilizing cyber attacks below the threshold of armed conflict, may not be enough in cases where these activities are having strategic effects to degrade the U.S. power base.

This perspective is shared by the Defense Science Board Taskforce on Cyber Deterrence, which warns against a large range of actors and cyber activities that "individually are only slightly disruptive or destructive, but which over time can subject the United States to 'death by 1,000 hacks' and impose cumulatively high costs while undermining our credibility of response to more impactful individual attacks."[2]

To achieve cyberspace superiority in an environment where actors operating below the threshold of armed conflict can nonetheless have strategic effects against the United States, the Cyber Command Vision proposes a three-pronged approach:

1. Increase resiliency
2. Defend forward, closer to the source of attacks
3. Persistently contest malicious cyberspace actors

Notably, this approach intentionally moves away from deterrence. In fact, deterrence is hardly mentioned in the Vision at all. Deterrence is not the end (or even the means) of the strategy; rather, it is relegated to a positive side effect. If the United States achieves and maintains superiority in cyberspace through increased resiliency, defending forward, and persistent engagement, then adversaries are more likely to be deterred from acting against our interests.

Cyber persistence is central to the new Vision. It defines cyber persistence as "the continuous ability to anticipate the adversary's vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions." The proposed methods for persistence range from stopping malicious activity before it reaches our networks to forcing adversaries to focus more on their own defense: "Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks."[23] The Vision states that a "high-demand, low density maneuver force" will be used to counter highly capable state actors and violent extremists. For other actors, increased resiliency is the main strategy for countering threats.

The trend in U.S. policy away from deterrence by denial and towards countering cyber threats through persistent engagement with adversaries mirrors the same trend occurring in the academic literature on deterrence in cyberspace. The general consensus, among scholars and policymakers, is that deterrence by denial is insufficient, and restraint on the part of the U.S. in responding to cyber attacks has not worked to stop (and may, in fact, have resulted in) a greater number of actors seeking to degrade the strategic power base of the United States through attacks below the threshold of armed conflict. The Command Vision proposes a solution, cyber persistence, but exactly how this solution will be implemented has not yet been determined.

3.3. International law and the problem of thresholds

U.S. policy neatly divides cyber operations into two categories, those that are above the threshold of the use of force, and those that are below it. There are good reasons for doing so.

International law restricts operations and activities (including in cyberspace) against other states, and force can only be employed in certain situations. During peacetime, nations have a right to self-defense when they come under attack. States are generally prohibited from intervening coercively in another state's affairs and from violating state sovereignty or territorial integrity. During war, the Law of Armed Conflict and International Humanitarian Law apply. The use of force must meet certain criteria, such as distinction between civilian and military targets and only using weapons that can be targeted and controlled in their effects, as opposed to having indiscriminate effects, like biological weapons, for example. Therefore, there are already well-established international norms defining what constitutes "armed attacks" or "acts of war" that trigger the relevance of the Law of Armed Conflict.

How do we know when a cyber attack reaches the level of armed attack? We have seen that many believe that above the threshold of armed attack, deterrence (by punishment) remains intact. Below this threshold, there are too many actors, and so a lack of consistent enforcement of consequences results in a breakdown of deterrence. But in practical terms, what does this threshold look like? If a cyber attack results in a power outage of a U.S. city for 24 hours, and one person dies as a result, does this constitute armed attack? What if ten people die, or one hundred? What if no one dies, but $100 million in damages are done?

Schneider and her colleagues conducted a series of wargaming exercises with senior leaders from fifteen critical infrastructure sectors, state and federal government officials, and other experts to ask the questions "When do attacks against U.S. critical infrastructure rise to the level of national security threats?" and "When do these national security threats warrant action by the Department of Defense and in what capacity?"[24] Participants generally agreed that no amount of economic damage was high enough to trigger the perception that a national security event had occurred. In contrast, participants viewed loss of even a single life as a national security event. Participants believed that the Department of Defense played a role primarily before attacks happen, through deterrence and counter threat operations, and after an attack had concluded, through retaliation.

Are cyber attacks perceived inherently different than "kinetic" attacks that have the same physical effects? Kreps and Schneider investigated this question through surveys and found that the American public is less likely to support retaliation to a cyber attack than to a kinetic attack, even when the physical effects of the attack are held constant.[25] The ramifications for deterrence are clear – if the American public is hesitant to respond to cyber attacks, then the U.S., as a constitutional republic, may be perceived to lack the political will required to consistently impose consequences for attacks.

Even if we can agree on a threshold, strategic attacks are occurring below the threshold of armed attack. How does international law apply to these conflicts? Actors in this space are not necessarily limited to state actors, and so international norms and laws may not apply. Still, the United States is constrained by international norms and laws when it responds, and this affects deterrence. Potential adversaries have certain expectations about how the United States will (or more precisely will *not*) respond to certain kinds of attacks.

The question of how to discuss and define thresholds is one that the Civilian Cyber Strategic Initiative grappled with throughout the year, and we believe further discussion is merited here at the laboratory and by policymakers at the national level. We believe that there are a number of metrics around which discussions of thresholds can occur, including economic impact, loss of

life or casualties, loss of confidence in government or elections, visibility to the public, interest by the media (i.e. shock value), violation of moral or ethical norms, and there may be many more.

3.4. The role of uncertainty in deterring cyber adversaries

One obvious problem with having clear thresholds is that adversaries will constantly operate just below the level where they think consequences will be imposed. There is a case to be made for the important role that uncertainty, often called strategic ambiguity, plays in deterrence. Strategic ambiguity has its roots in a prominent debate that occurred during the Cold War. The central question of that debate was: Does uncertainty improve the effectiveness of deterrence?

There were two schools of thought on this question. Herman Kahn argued that deterrence is best achieved if the adversary knows with absolute certainty what consequences will occur if they take the action that the deterrer wants to prevent. Kahn believed that "uncertainty can push a gambling opponent in the direction of war"[26] rather than in the direction of restraint and de-escalation. Rational actor theory hinges on a common understanding between two states about the costs and benefits of their actions. But can this really be achieved? And if the answer is *no*, where does that leave deterrence theory?

Thomas Schelling argued that uncertainty is unavoidable:

> Not everybody is always in his right mind. Not all the frontiers and thresholds are precisely defined, fully reliable, and known to be so beyond the least temptation to test them out, to explore for loopholes, or to take a chance that they might be disconnected this time. Violence, especially in war, is a confused and uncertain activity, highly unpredictable, depending on decisions made by fallible human beings organized into imperfect governments depending on fallible communications and warning systems and on the untested performance of people and equipment. It is furthermore a hotheaded activity, in which commitments and reputations can develop a momentum of their own.[27]

Uncertainty is unavoidable, but deterrence theory does not suffer for it, Schelling believed. Rational actors are perfectly capable of factoring irrationality on the part of their opponent into their decisions. Instead of knowing with one hundred percent certainty that an unacceptable consequence will be imposed on me for some proscribed action, what if there were only a ten percent chance, or a five percent chance? If the consequence is high enough, even a small chance that it will occur may serve to deter unwanted actions.

Schelling's school of thought came to dominate the nuclear domain, and strategic ambiguity is standing U.S. policy when it comes to using nuclear weapons. For example, the 2018 Nuclear Posture Review states that the purpose of nuclear weapons is not simply to deter nuclear use against the United States and its allies, but also to deter a range of other "strategic non-nuclear attacks" including attacks on civilian critical infrastructure.[7]

Libicki provides a succinct summary for the requirements of deterrence in in uncertain conditions: "The raw calculus of deterrence is fairly straightforward: The lower the odds of getting caught, the higher the penalty required to convince potential attackers that what they might achieve is not worth the cost." However, he cautions against applying this logic to the cyber domain: "Unfortunately, the higher the penalty for any one cyberattack, the greater the

odds that the punishment will be viewed as disproportionate"[3] and therefore, not credible. We glean additional warnings from the realm of criminal deterrence, where empirical evidence has shown that deterrence outcomes are improved by increasing the certainty of punishment, and that the severity of punishment does not increase deterrence effectiveness.[28-29]

3.5. Thresholds may increase deterrence effectiveness

Despite the potential, though debatable, benefits of employing strategic ambiguity in cyberspace, we argue that the establishment of thresholds may serve to improve the effectiveness of deterrence of cyber adversaries, because they help to clarify exactly what we would like to deter, and how often.

Skeptics of deterrence theory's applicability to cyberspace typically site several major challenges, many of which will be discussed in Section 4. Proponents of applying deterrence to conflict in cyber space argue that deterrence does not necessarily apply at all levels of conflict. Just as nuclear weapons are not intended to deter conflict at all levels, only at the highest range of consequences, so too may deterrence of cyber adversaries only be effective for certain types of conflict. Two major challenges often cited by skeptics include difficulties of rapid, high-confidence attack attribution, and the sheer number of actors operating in cyberspace. The counter-argument is that, given enough time and resources, many attacks are attributable.[30-31] Furthermore, as the severity and sophistication of a cyber attack increases, the number of actors capable of carrying out that threat decreases, which also aids in attribution.

Figure 2 shows a hypothetical categorization of deterrence policy goals based on cyber attack severity, with notional functions describing attribution and the number of capable actors. As attack severity increases, the number of actors capable of carrying out such an attack decreases. The actual shape of this function is not known, and what is shown is notional. Moreover, the number of actors at higher capability levels is likely increasing over time (grey dotted line). The blue dotted line conveys the hypothesis that as attack severity increases, so does our ability for high-confidence attribution. Again, the true shape of the function is not known. However, if these two hypotheses are true, that increasing attack severity correlates positively with our ability to attribute and negatively with the number of capable actors, then deterrence by punishment becomes more likely to succeed at the highest severity levels – precisely where we need it the most.

We cannot (and do not) deter cyber attacks at all levels of severity. There is some threshold for attack severity above which we would want to deter all attacks (red). Deterrence by punishment is most applicable in this range, although denial, entanglement, and norms are also active. Below this threshold, we want to decrease the frequency of successful attacks, but we may not be able to deter everything (yellow). Here, punishment plays a smaller role than denial, entanglement, and norms. At the lowest end of the spectrum, we may choose not to invest resources in deterring attacks at all. The precise location of these thresholds is up for debate and is a very serious and difficult question that policymakers must contend with, even if the answers are never publicized. Yet we maintain that in order to craft effective deterrence policy, you must know what you want to be able to deter.

The consensus appears to be that below the threshold for the use of armed force, however difficult it may be to define that threshold, deterrence begins to fail. But it is precisely this realm of conflict that adversaries seek to exploit, because they can have strategic effects below the

level of kinetic retaliation. If deterrence above a certain threshold succeeds, and deterrence below that threshold fails, the question then becomes, why does it fail? And how can we improve our ability to deter these types of attacks? These are the subjects of the following two sections.

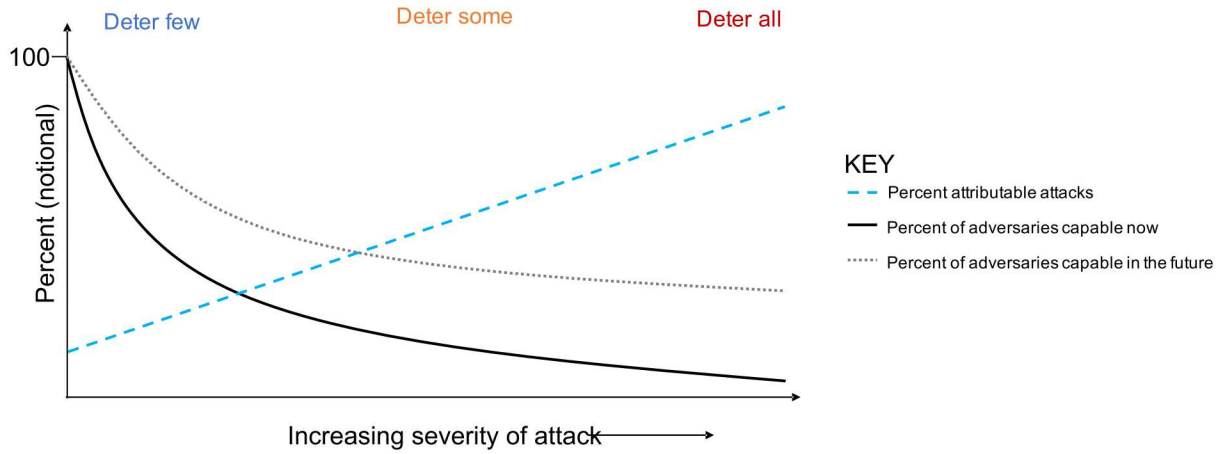


Figure 2. Notional categories for crafting deterrence policy goals

4. UNIQUE CHALLENGES OF DETERRENCE IN CYBERSPACE

Both Libicki[3] and Fischerkeller and Harknett[12] discuss why deterrence in cyberspace is fundamentally different than nuclear deterrence specifically and military deterrence in general. Below, we summarize several of their observations, along with additional insight collected from our discussions with subject matter experts.

4.1. Inherent domain characteristics

The prefix *cyber* often refers to a variety of digital networks or wireless systems, including anything involving computers and the Internet. While the U.S. military often refers to it as a *domain* distinct from other domains (land, air, sea, space), it is also a tool or an asset that can enhance operations of other tools and assets within each of these domains. The Department of Defense has defined *cyberspace* as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[32] However, even broader definitions exist. Some argue that cyberspace is not a domain, but a substrate, "an underlying layer on which modern society is built. Cyberspace uniquely underpins all warfighting domains."[33]

How cyberspace is perceived by different actors necessarily impacts deterrence. As Schneider points out, "imagine, for example, examining a tank's ability to deter land, sea, and air conventional operations versus a highway's ability to deter those same operations."[14]

If we assume that cyber is a domain, it possesses certain unique domain characteristics compared to the physical domains. Digital systems are simultaneously *deterministic* and *unpredictable*. Deterministic refers to the consistent manipulation of input data by a series of logic controllers to output the same result every time (given the same input). If adversaries know the exact nature of the system they are targeting, they can design an attack at home on their own system that they know will function a certain way in the target system. But the digital domain is also inherently unpredictable. In physical domains, we can make predictions about the probability or likelihood of certain outcomes because many observables are "smooth" or "reducible" and can be approximated despite a lack of knowing exact inputs. We know, for example, that anything in physical spaces is subject to the laws of physics, and these constraints help bound the problem.

In contrast, digital computers are highly nonlinear physical systems – we cannot easily predict the outcome of untested digital inputs. The number of possible digital inputs (potential attacks) is exponentially large, and so we cannot possibly test them all. And it is much more difficult to bound the worst-case response of a digital system to a targeted attack than for a physical system. For digital systems, we face an inherent tradeoff. They can execute complex behaviors very reliably, but the full space of those behaviors is much more difficult to bound in advance. Therefore, we cannot easily say what the probability is that a certain class of attacks will result in a particular outcome, which means that cyber systems are inherently unpredictable.

Another inherent characteristic of cyberspace is what Fischerkeller and Harknett call *constant contact*.[12] Constant contact describes the interaction between all cyber actors – that they are always and everywhere in contact with each other. Constant contact is the result of several composite cyber domain characteristics, including the low cost or low barrier to entry leading to a multitude of actors, a lack of territorial borders, and rapid contact.

Becoming an actor in the cyber domain is relatively inexpensive, and there is little to no barrier to entry for new actors. This leads to a multitude of different actors and potential adversaries, that possess a spectrum of capabilities, motivations, and intentions. Most other military domains have relatively higher costs or higher barriers associated with entry. Establishing a submarine fleet or a standing land army, enriching and weaponizing uranium, launching a satellite – these all take significant resources and expertise that are not available to everyone. But almost anyone can launch cyber attacks. The sheer number of actors degrades deterrence effectiveness. If there are too many perpetrators to prosecute, then consequences cannot be imposed consistently, and adversaries learn that they can act with impunity. Prosecuting and punishing only a small fraction of the perpetrators does not signal a credible deterrent threat.

The internet connects everyone around the globe almost instantly; therefore, there is rapid contact between actors and their targets. Contact through physical spaces (air, land, sea, space), takes time – at least a few minutes or hours. Furthermore, in cyberspace, there are no recognized geographical or territorial borders. Lack of territorial borders removes certain norms associated with state sovereignty and territorial integrity, which may degrade the ability of states to send deterrence signals and to recognize signals that are being sent by others.

4.2. Attack detection

Cyber attacks, exploits, and intrusions are difficult to detect. Even in cases where cyber activities have physical effects, it may be difficult to know that the effects are due to adversarial activity, as opposed to human or systematic error, or an accident. Once effects are known it may not be obvious that the activity originated in cyberspace. In some cases, detection of an attack can take months or even years. Evidence of the attack may take a long time to surface. The effects themselves may be hidden or may take a long time to materialize.

The difficulty of detecting cyber activity stands in marked contrast to the nuclear domain. If a nuclear device is detonated, decision makers would know within a matter of minutes what has occurred. For attack detection, cyber activities are therefore less like nuclear and more like human intelligence or espionage, in which an adversary can collect information for years before being discovered (if they are discovered at all), or perhaps a biological weapons attack disguised to look like a naturally occurring epidemic.

Slow and uncertain detection times influence deterrence because they increase the time between the precipitating event and the response. Presumably, the greater amount of time between an attack and the response, the more deterrence effectiveness is degraded. However, the nature of this degradation of deterrence effectiveness over time is not known, and would be a rich area for further study.

4.3. Attack attribution

The difficulty of attributing cyber activity is one of the most significant barriers to applying deterrence theory in cyberspace. Libicki aptly describes several reasons why attribution of cyber activity is difficult: “Computers do not leave distinct physical evidence behind. The world contains billions of nearly identical machines capable of sending nearly identical packets. Attacks can come from anywhere. State-sponsored hackers could operate from a cybercafé, a public library with Wi-Fi access, or a cutout…Packets can be bounced through multiple machines on their way to the target. They can be routed through a bot that only needs to erase the

packet's originating address and substitute its own to mask the true origin. Attacks can be implemented beforehand in any machine that has been compromised."[3] It is easy to conceal one's identity in cyber space, or to masquerade as someone else. On the web, anonymity is enshrined as essential to privacy and confidentiality of personal information. We cannot change the ability of actors to conceal their identity in cyberspace without fundamentally changing the structure of the Internet to reduce anonymity.

As discussed in Section 2, deterrence by punishment, deterrence by norms, punctuated deterrence, and cumulative deterrence concepts all rely heavily on being able to attribute cyber attacks. If it is not known who is behind a cyber attack or where it originated, it is not possible to reliably respond to the cyber attack. Many deterrence skeptics claim that attribution in cyberspace is impossible. However, there are several scholars that contend that attribution is not impossible, but it may be difficult, and it could take a very long time.[30-31] If this is the case, then the same question arises here as for long detection times for malicious cyber activities: how is deterrence effectiveness degraded when the attack and the response are separated in time?

Attribution is much more complex than answering the question "*who did it?*". A series of questions arise:

1. *Who did it?* – As Lin describes,[30] there are multiple potential answers to this question, and answering them does not necessarily clarify who should be held responsible. Which machine did the attack originate from? Who is the person pushing the keys on that machine? Who owns that machine? Where is the machine? Who ordered the attack to be carried out? One could accurately answer all of these questions, but there is no legal consensus for who can or should be held responsible.

   This question can partly be answered by knowing what the goals of attribution are. If the goal is to stop the attack, you only need to know which machine the attack is coming from. It does not matter who is pushing the keys or who ordered the attack. However, deterrence may operate at multiple levels. We might want to deter the actors pushing the keys. If they know that certain systems are better protected, they may move along the path of least resistance to attack other systems. Alternatively, we might want to deter the actor who ordered the attack, which requires understanding a completely different adversarial cost/benefit calculation.

   Complications surrounding the question *who did it?* are not necessarily unique to cyber. We can imagine a scenario where a pilot from Country A is flying a bomber with insignia from Country B and bombs a city under the orders of Country C. Who is responsible? The major difference here is that the international community has established norms that countries are responsible for their bomber aircraft. The question we all ask then is not *who did it?* but *why did Country B lose control of their bomber?* The burden of proof is shifted onto Country B. Such norms do not exist for cyberspace.

2. *Did the adversary intend these effects?* – As will be discussed below, the effects of cyber attacks are often uncertain. When a cyber system behaves abnormally, it could be due to bad software, human or random error, or a natural disaster.[3] Even if we know that a certain cyber event is due to malicious activity, we may not know what the intent of the adversary is in conducting that activity. "A cyber attack that causes a minor

power outage could be a warning shot, a failed attempt at a major strategic network breach, or an inadvertent result of reconnaissance," according to Buchanan and Rid.[34]

3. *Can attribution be proved to others?* – In order for deterrence to be established or strengthened through response, attribution must be proven to several parties. Nye describes three relevant but distinct audiences that must be considered when attributing cyber attacks.[8] The first is the defending government, which requires a certain burden of proof from its intelligence agencies and other forensic evidence gathered in order to respond to the attack. The second audience is the attacking government or party, which knows that it is guilty but does not know the level of confidence that the defending government has in their case for attribution. If the attacking party believes that the defending party is biased and would have attributed any malicious activity to them anyway regardless of the amount of evidence available, deterrence is not strengthened. The third audience is the domestic and international public that must be convinced of the justness of retaliation on the part of the defender.

Depending on the situation and on the goals for attribution, the degree to which making the case to each of these audiences may vary. There may be cases where we do not need or want to openly associate our response to precipitating events, although this might not aid signaling for deterrence purposes. There may be ways to signal or demonstrate resolve without making a response in a public manner. But even in these cases, convincing the first two audiences is still necessary. Uncertainty may also play a role here. How confident do we need to be in our attribution to be able to respond? Can we capitalize on our uncertainty, and the perceived uncertainty in the minds of our adversaries, to deter without achieving absolutely certain attribution? Is proving attribution with certainty necessary for responding with the intent to deter others?

Certain challenges arise when sharing information about attribution. The evidence of the attack and the methods of may be classified, as they may reveal our vulnerabilities or certain intelligence capabilities. There is also the risk that we could misattribute attacks. While it is tempting to assume that our ability to attribute will improve over time as technology improves, this is not necessarily the case. The ability to conceal or hide one's identity in cyberspace may outpace attribution capabilities.

4.4. Escalation control across domains

Crafting responses to cyber attacks is inherently a cross-domain deterrence challenge.[4, 35-37] Schelling argued that "like deters like," that is, deterrence is more likely to be effective if the characteristics of the response match those of the initial attack as closely as possible. Therefore, expanding a conflict into other domains may be viewed as inherently escalatory. However, it may also be the case that decision makers choose to respond across domains in an effort to de-escalate a crisis, as was the case in the Cuban Missile Crisis.[38] Regardless, proportionality is probably harder to achieve when responding across domains. It seems more likely that the response will be either inadvertently escalatory or de-escalatory than it will be exactly proportional.

4.5. Asymmetric vulnerability

In cyberspace, the United States is more vulnerable than most of its potential adversaries. For the United States, cyberspace is more of a vulnerability than an asset when it comes to deterrence. The United States has a larger attack "surface area" than other nations. More aspects of our society are supported by cyber systems, and we are uniquely dependent on them as well.

Hjortdal describes three ways that great power states are incentivized to use cyber operations against the United States based on a perception of asymmetric vulnerabilities and gains: 1) to obtain a deterrent threat through infiltration of critical infrastructure, 2) to obtain a military advantage through military espionage, and 3) to gain an economic advantage through industrial espionage.[39] Clark and Knake argue that "the U.S. probably should be deterred from initiating large-scale cyber warfare for fear of the asymmetrical effects that retaliation could have on American networks."[40] Therefore, the disproportionately high vulnerability of the United States limits its ability to act in cyberspace and to respond to malicious cyber incidents.

4.6. Lack of international norms and laws

Section 3.3 provided a brief discussion of the progress that has been made in applying existing international law to cyberspace. Compared to other domains, there has been relatively little time for norms and laws to solidify for cyberspace. In the United Nations, initial debates began in the late 1990s. At first there was reluctance to apply existing international law to cyberspace, and many called for an entirely new framework. However, the UN Group of Governmental Experts (UNGGE) met in 2015 and decided that international law does apply in cyberspace. Since then, the GGE has failed to meet consensus on *how* the law applies – that is, on what types of attacks constitute armed attack for which a response using force is justified.

It is clear that not all states agree about which aspects of cyberspace should be protected by international law. Many states believe in protecting Internet freedom, human rights, and cybersecurity. Others tend to emphasize state sovereignty, Internet governance, and information security. Norms proposed by one state are often viewed by another as restrictive of human rights, fostering censorship, or preventing freedom of action in cyberspace. One reason the establishment of norms could be more difficult in cyberspace as opposed to other domains is that norms governing conflict in physical domains center around concepts of state sovereignty and the violation of territorial borders, neither of which exists in the same way in cyberspace.[12]

Fischerkeller and Harknett caution that while the United States and its allies have so far sought to develop norms for cyber behavior based on principles of operational restraint, other actors are finding that restraint does not serve their interests, and more aggressive actions do. As norms are developed through behavior, they will be dominated by those who are taking the most actions in cyberspace. Therefore, the United States and others who operate on a principle of restraint are allowing norms to be defined by those who disagree: "Undoubtedly, these actors have recognized that when the time comes for international discourse regarding codification, those who operationally dominate the domain will be in the strongest position to argue for norms supporting their positions."[12] The implication is that if the United States continues to adhere to a doctrine of cyber restraint, it will not be in a strong position to define the norms of conflict in the domain.

Deterrence of state actors partially relies on a common understanding of international norms and laws. At a minimum, potential adversaries of the United States may expect the United States to be constrained by its understanding of international law. Beyond specifics, deterrence would be strengthened if both actors understand what types of behavior in cyberspace constitutes an armed attack that would justify a kinetic retaliation from the perspective of the international community. At the moment, those norms simply do not exist and are still rapidly evolving for each state, potentially in divergent ways.

Additionally, since strategically significant cyber activity is occurring below the threshold of armed attack, it is equally important for norms to develop in this space as well. Damage caused by a cyber operation that constitutes armed attack is fundamentally different from damage caused by espionage, sabotage, and subversion, all of which might occur below the threshold of armed attack.[12] Norms must also be developed for activities and conflict that do not trigger the Law of Armed Conflict.

4.7. Lack of domestic laws and private sector regulation

What is or should be the role of the federal government in responding to cyber attacks or threats to the private sector? To what degree does the responsibility for cybersecurity and system resiliency lie with the private sector? If a private corporation is hacked, are they legally allowed to conduct a forensic investigation, reach a determination on attribution, and retaliate or "hack back"? What if they are in a better position to do so than the federal government? And what effect does all of this have on deterrence effectiveness?

As previously discussed, some degree of uncertainty about *who* will respond (the federal government versus a private corporation) does not necessarily render deterrence ineffective, but it might change the primary mechanisms through which deterrence operates. In contrast to nuclear and other military domains, cyber lies across all agencies of the federal government (and state and local governments), as well as the private sector. This means that decisions about cybersecurity are highly decentralized and heterogeneous. Decentralized decision-making will decrease the certainty about whether and how we will respond to certain types of cyber activities.

4.8. Uncertain effects of cyber weapons

The effects and outcomes of some cyber operations and activities are hard to control. The effects of a cyberweapon are not necessarily limited to the intended target. The potential for uncertain effects of cyber weapons has important ramifications for deterrence both when one is the victim of an attack and when one is responding in retaliation for a cyber attack using an offensive cyber operation.

1) A victim of a cyber attack will not know whether their adversary intended to produce the effects that occurred, or whether their adversary intended milder (or more severe) outcomes. This makes it difficult to know how to respond in a proportional manner.

2) An actor that means to respond to a cyber attack using a cyber operation will not know for sure if the intended effects of their actions will be proportional to the initial event, or painful enough to induce their adversary not to act in the first place. Additionally, if the effects are indiscriminate enough, they could harm the deterrer through entanglement or through political blowback.

Uncertain effects are not a challenge that only applies in cyberspace. In fact, many argue that, in contrast to kinetic operations, the effects of cyber operations can be far *more* controlled to limit collateral damage, if that is intended by the actor. There appear to be both options: precision attacks that have certain effects on limited targets, and broad scope attacks that have uncertain effects on unlimited targets, with a spectrum of options in between. Perhaps that broad spectrum is what makes cyber different than other domains. The effect of this characteristic on deterrence effectiveness is not known, and would benefit from further consideration.

4.9. Blurred lines between offense and defense

In physical domains, defense occurs on one's own territory, and offense is concerned with what may happen on another's territory. In a domain of constant contact, there are no territorial boundaries. Defense may start in another's networks, and offense may start in one's own networks. As an example, consider efforts to improve attribution. One method of attribution is to collect evidence and information to determine who conducted an attack (or to rule out who did not). A second option is to monitor the systems of potential adversaries for suspicious activity related to any attacks they might conduct. This would provide even higher confidence attribution. However, this type of espionage may look less like defense and more like offense to one's adversary. The initial stages of both espionage (Computer Network Exploitation, CNE) and disruption (Computer Network Attack, CAN) can look very similar. "Preparing the battlefield" for a larger scale attack might appear very similarly to espionage or intelligence gathering for purely defensive purposes.

The blurred lines between offense and defense complicate deterrence. For example, even if states can agree that cyber espionage does not constitute armed attack and network disruption does, can we easily tell the difference every time? Establishing a robust defense, and "defending forward" to stop attacks before they reach our own networks are both important aspects of deterrence by denial. To an adversary, however, these actions may look far more aggressive, and the potential for misunderstanding and miscommunication is high.

5. REFERENCES

1. Schelling, T. C., *Arms and Influence*. Yale University Press: New Haven, CT, 1966.
2. *Task Force on Cyber Deterrence*; Department of Defense Defense Science Board: 2017.
3. Libicki, M. C., *Cyberdeterrence and Cyberwar*. RAND Corporation: Santa Monica, 2009; p 214.
4. Mallory, K. *New Challenges in Cross Domain Deterrence*; PE-259-OSD; RAND Corporation: 2081.
5. Bunn, M. E. *Can Deterrence Be Tailored?*; Institute for National Strategic Studies, National Defense University: 2007; pp 1-8.
6. Bracken, P., The Cyber Threat to Nuclear Stability. *Orbis* **2016,** *60* (2), 188-203.
7. Nuclear Posture Review. Defense, U. S. D. o., Ed. 2018.
8. Nye, J. S. J., Deterrence and Dissuasion in Cyberspace. *International Security* **2017,** *41* (3), 44-71.
9. Tor, U., 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies* **2015,** *40* (1-2), 92-117.
10. Reinhardt, J., Thoughts on Deterrence Asymmetries Across Domains. Sandia National Laboratories, 2016.
11. Kello, L., *The Virtual Weapon and International Order*. Yale University Press: New Haven, CT, 2017.
12. Fischerkeller, M. P.; Harknett, R. J., Deterrence is Not a Credible Strategy for Cyberspace. *Orbis* **2017,** *61* (3), 381-393.
13. Brodie, B.; Dunn, F. S.; Wolfers, A.; Corbett, P. E.; Fox, W. T. R., *The Absolute Weapon: Atomic Power and World Order*. Harcourt, Brace and Co.: New York, NY, 1946.
14. Schneider, J., Cyber and Cross Domain Deterrence: Deterring Within and From Cyberspace. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Gartzke, E.; Lindsay, J., Eds. Oxford University Press: 2019.
15. Lynn, W. J. I., Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs* **2010,** (September/October 2010).
16. The Comprehensive National Cybersecurity Initiative. House, T. W., Ed. Washington, D.C., 2009.
17. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. House, T. W., Ed. Washington, D.C., 2011.
18. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. House, T. W., Ed. Washington, D.C., 2013.
19. The Department of Defense Cyber Strategy. Defense, U. S. D. o., Ed. Washington, D.C., 2015.
20. National Security Strategy of the United States of America. House, T. W., Ed. Washington, D.C., 2017.
21. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. House, T. W., Ed. 2017.
22. *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*; 2018.
23. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command. Command, U. S. C., Ed. 2018.

24. Schneider, J.; Schechter, B.; Shaffer, R. *Navy – Private Sector Critical Infrastructure War Game Report 2017*; United States Naval War College: 2017.
25. Kreps, S.; Schneider, J., Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics. *Social Science Research Network Electronic Journal* **2018**.
26. Delpech, T. r. s., *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy*. RAND Corporation: Santa Monica, 2012.
27. Freedman, L., *The Evolution of Nuclear Strategy*. 3rd ed.; Palgrave Macmillan: New York, NY, 2003.
28. Nagin, D. S., Deterrence in the Twenty-First Century. *Crime and Justice* **2013,** *42* (1), 199-263.
29. Paternoster, R., How Much Do We Really Know about Criminal Deterrence? *The Journal of Law & Criminology* **2010,** *100* (3), 765-823.
30. Lin, H. *Attribution of Malicious Cyber Incidents: From Soup to Nuts*; Stanford University Hoover Institute, 2016.
31. Lindsay, J. R., Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity* **2015**.
32. Cyberspace Operations. Staff, J. C. o., Ed. 2018.
33. Dombrowski, P.; Demchak, C. C., Cyber War, Cybered Conflict, and the Maritime Domain. *Naval War College Review* **2014,** *67* (2), 1-27.
34. Rid, T.; Buchanan, B., Attributing Cyber Attacks. *Journal of Strategic Studies* **2014,** *38* (1-2), 4-37.
35. Lewis, J. A. *Cross-Domain Deterrence and Credible Threats*; Center for Strategic and International Studies: 2010.
36. Lindsay, J.; Gartzke, E., Cross-Domain Deterrence as a Practical Problem and Theoretical Concept. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Lindsay, J.; Gartzke, E., Eds. Oxford University Press: 2019.
37. Manzo, V., Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit? *Joint Force Quarterly* **2012,** *66* (3).
38. Nacht, M.; Schuster, P.; Uribe, E., Cross-Domain Deterrence in American Foreign Policy. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, Lindsay, J.; Gartzke, E., Eds. Oxford University Press: 2019.
39. Hjortdal, M., China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* **2011,** *4* (2), 1-24.
40. Clarke, R. A.; Knake, R. K., *Cyber War: The Next Threat to National Security and What To Do About It*. HarperCollins: New York, NY, 2010.

DISTRIBUTION

1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories