SANDIA REPORT
SAND2020-9589
September 2020

Sandia National Laboratories

Resilient Energy Systems and Cyber Deterrence and Resilience Strategic Initiatives

Cyber Resilience as a Deterrence Strategy

Ann E. Hammer, Trisha H. Miller, Eva C. Uribe

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

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & 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/

The work described in this report was performed as part of the Cyber Deterrence and Resilience Strategic Initiative, an internally funded effort at Sandia National Laboratories. Strategic initiatives crosscut existing programs at the lab and fund exploratory studies that identify opportunities to inform the national dialogue on emerging national security threats and challenges. Contributing authors are from the Systems Research and Analysis Group, which engages multidisciplinary teams to investigate national security solutions in complex systems, through consideration of technology, policy, operations, and human factors. The views expressed within this publication are solely those of the authors and do not necessarily represent the views of Sandia National Laboratories or any other agency or sponsor. This paper is approved for unlimited release as SAND2020-5016.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

ABSTRACT

This paper was written by the Cyber Deterrence and Resilience Strategic Initiative in partnership with the Resilience Energy Systems Strategic Initiative. Resilience and deterrence are both part of a comprehensive cyber strategy where tactics may overlap across defense, resilience, deterrence, and other strategic spaces. This paper explores how building resiliency in cyberspace can not only serve to strengthen the defender's posture and capabilities in a general sense but also deter adversaries from attacking.

ACKNOWLEDGEMENTS

We would like to thank all of the members of the Sandia National Laboratories Cyber Deterrence and Resilience Strategic Initiative (CDRSI) for their contributions to this paper, including Jeffrey J. Apolis, Benjamin J. Bonin, Ruby E. Booth, Robert D. Forrest, Ryan Jacobson, David Johnson, Ahmad Jrad, Michael F. Minner, Jason C. Reinhardt, Kiril Taskov, Nerayo P. Teclemariam, William Waugaman, and Lynn I. Yang. We acknowledge the support and guidance of Heidi Ammerlahn, Richard Griffith, and Jennifer Gaudioso.

CONTENTS

1. Introduction 9
2. Historical Context: Deterrence by Denial 11
3. Role of Cyber Resilience in Deterrence 12
   3.1. Unique Cyber Domain Challenges and Deterrence through Resiliency 14
4. Connections Between Deterrence and Resilience in Current Strategy Documents 15
5. Conclusion: Cyber Resilience as a Deterrent 16
Appendix A. Deterrence Requirements for Various Types of Deterrence Strategies[2] 17

LIST OF FIGURES

Figure 1. Notional Components of a Comprehensive Cyber Strategy 7
Figure 2. Breakdown of various deterrence mechanisms by time of cost imposition or denial of benefits relative to the attack phase[2] 13
Figure 3. The 4 C's of Deterrence through Resilience 13

LIST OF TABLES

Table 1. Deterrence by Denial in the Cyber Domain 14

This page left blank

EXECUTIVE SUMMARY

Cyberattacks can result in economic losses, damage to infrastructure, loss of service and functionality, human injury or death, and/or impact national security[1]. To compound the breadth of potential consequences from an attack, international regulation, standards, and norms of behavior are lacking in cyberspace, complicating attribution and retaliation. Resilience of key systems to degradation and destruction by cyber attackers is essential, yet resilience also serves as a very important element to deter adversaries.

Cyber resilience concepts are consistent with fundamental deterrence concepts. Deterrence is the creation of conditions where adversaries are dissuaded from acting because they perceive that the costs are unacceptably high, or the benefits are insufficient. Key cyber resilience concepts include:

- Have systems in place that minimize the consequences or impact of an attack
- Sustain operations throughout and after an attack
- Recover and adapt to new conditions after an attack

In order for these three system attributes to deter potential attackers, they must be *signaled or demonstrated* such that the attacker perceives fewer gains and/or a need to expend more resources to achieve the same desired effect.

This paper explores how building resiliency in cyberspace can not only serve to strengthen the defender's posture and capabilities in a general sense but also deter adversaries from attacking. Resilience and deterrence are both part of a comprehensive cyber strategy where tactics may overlap across defense, resilience, deterrence, and other strategic spaces. (Figure 1)

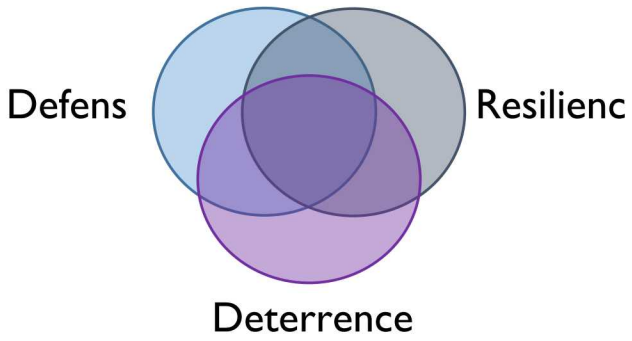

Figure 1. Notional Components of a Comprehensive Cyber Strategy

Perfect defense in cyberspace is essentially impossible[2], further emphasizing the need to build resiliency and strengthen deterrence capabilities. There is not yet consensus on the role of deterrence in cyberspace, but the objective is to put forth some of the thinking that has been done on the

[1] National Security Strategy of the United States of America, December 2017 https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[2] Department of Defense, Defense Science Board – Task Force on Cyber Deterrence, February 2017 https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

concept and invite further discussion on the integration of deterrence and resilience in this domain. The challenges and strategies described apply across the government and private sector.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
NATO	North Atlantic Treaty Organization
SNL	Sandia National Laboratories
DHS	Department of Homeland Security
CDRSI	Cyber Deterrence and Resilience Strategic Initiative
DoD	Department of Defense
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
DSB	Defense Science Board
CROWS	Cyber Resiliency Office for Weapons Systems

1. INTRODUCTION

This paper explores the relationship between deterrence and resilience in the cyber domain by defining key concepts, highlighting aspects of historical deterrence theory to demonstrate the role of resilience, and exploring how resilience can play a significant role in deterring cyberattacks. The objective is to encourage further discussion and progress towards integrating deterrence and resilience as well as to evaluate how to implement the concepts across the government and private sector partners.

Cyberattacks can result in economic losses, damage to infrastructure, loss of service and functionality, human injury or death and/or impact national security. To compound the breadth of potential consequences from an attack, international regulation, standards, and norms of behavior are lacking in cyberspace, complicating attribution and retaliation. Resilience of key systems to degradation and destruction by cyber attackers is essential, yet resilience also serves as a very important element to deter adversaries. Perfect defense in the cyber domain is effectively impossible; attackers only have to find one way in, but defenders must guard an infinite number of entry points.

Definitions:

- NATO defines **deterrence**[3] as the threat of force in order to discourage an opponent from taking an unwelcome action. This can be achieved through the threat of retaliation (deterrence by punishment) or by denying the opponent's aims (deterrence by denial). We (Cyber Deterrence and Resilience Strategic Initiative [CDRSI] at Sandia National Laboratories[4]) (SNL) define deterrence more broadly to include not just the threat of force, but also by the prospect of unacceptable costs or insufficient benefits, whether or not that is achieved through the use of force or through some other mechanism (e.g. criminal indictment or economic sanctions).

- **Resilience**, as defined in Presidential Policy Directive -21 (PPD-21), is "the ability to prepare for and adapt to changing conditions and withstand and recovery rapidly from disruptions."[5]

Key cyber resilience concepts include:

- Having systems in place that minimize the consequences or impact of an attack
- Sustaining operations throughout and after an attack
- Recovering and adapting to new conditions after an attack

In order for these three system attributes to deter potential attackers, they must be signaled or demonstrated such that the attacker perceives fewer gains and/or a need to expend more resources to achieve the same desired effect.

---

[3] NATO REVIEW, April 20, 2015
https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html

[4] Sandia Report (SAND2020-5016) "Why does cyber deterrence fail, and when might it succeed? A framework for cyber scenario analysis". Uribe, Eva C. et.al. May 2020

[5] National Infrastructure Protection Plan [NIPP], 2013https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf

Resilience as a means of deterrence in the cyber domain is particularly important because rivals at present do not appear to be waging cyber war, but rather are using cyber methods to produce strategic effects below the threshold of armed conflict.[6] This provides rationale for resilient systems where the cost outweighs the desired effect and the ability to continue operations and recover make critical systems a less attractive target. Building cyber resiliency has a role both in resisting attacks as well as limiting effects and more swiftly recovering once attacked.

While deterrence is as old as war,[7] the lion's share of rigorous scholarship on this subject was conducted during the Cold War under the specter of full-scale nuclear war between great power rivals. During this era, resilience concepts were of central importance for guaranteeing the integrity and operational capacity of specific military systems, but less significant when applied to critical infrastructure and society more broadly. How does one withstand and rapidly recover from full-scale nuclear war? In the modern era, great powers, regional powers, rogue states, and non-state actors seek to compete, fight, and undermine their rivals' core strategic interests far below this level of conflict, even below the level of conventionally armed conflict. It is necessary to shift mindsets and capabilities to address the cyber threat and understand that resilience as a deterrent measure is uniquely important in the cyber domain.

Schneider[8] has described the difficulty of characterizing cyberspace as a *domain*, distinct from the physical military domains of land, air, sea, and space: "It might be administratively cohesive to think of cyberspace as a domain and deterrence, therefore, as across and through the cyberspace domain. However, the interpretation of cyberspace as a societal infrastructure that connects not only warfighting domains, but also civilian networks and functions significantly complicates the deterrence discussion. Cyberspace in this understanding becomes a target we must deter others from attacking… 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." What can be learned from this analogy? A tank's ability to deter is clear. It can swiftly impose costs on the battlefield. A highway cannot really deter, it is a more vulnerable target. However, a highway has appealing features; for one, it is part of a very large system of highways that undergirds society's ability to function and thrive during conflict and peacetime. That highway system is resilient; if one road fails, there are likely other routes that could achieve a similar objective. There are inexpensive "go-arounds." Additionally, highways enable us to build new tanks (and new everything else). They are the foundation on which everything else rests.

It must be noted that *resilience* exists independently of deterrence. Not every resiliency measure, policy, and/or technology put in place is intended to deter. However, resiliency principles (the ability to withstand an attack, operate through an attack, and recover functionality quickly) are compatible with fundamental deterrence concepts. Deterrence is the creation of conditions where adversaries are dissuaded from acting because they perceive that the costs are unacceptably high, or the benefits are insufficient. In order for resilient system attributes to deter potential attackers, they must be signaled or demonstrated such that the attacker perceives fewer gains and/or a need to expend more resources to achieve the same desired effect. Cost imposition and denial of benefits are two sides of the same coin. By denying the benefits of an attack through defensive measures or through

---

[6] 2018 USCYBERCOM Command Vision, "Achieve and Maintain Cyberspace Superiority."

[7] Sun Tzu wrote "The supreme art of war is subdue the enemy without fighting" in the 6th century BCE (Tzu, Sun; *The Art of War,* Translated by Samuel B. Grith. Oxford University Press, 1963). See also George Quester, *Deterrence Before Hiroshima*, Routledge, New York (2019).

[8] Jacquelyn Schneider, "Deterrence in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon Lindsay and Erik Gartzke (Oxford University Press, 2019)

resilience, a defender simultaneously raises the costs the attacker will sustain in order to achieve their intended effects.

2. HISTORICAL CONTEXT: DETERRENCE BY DENIAL

The first time "deterrence by denial" was coined as a term was by Glenn Snyder in 1960; this was in regard to the thinking around nuclear deterrence, but there are examples of this strategy being used long before the nuclear era. He defined it as "the capability to deny the other party any gains from the move to which is to be deterred." Denial is the defensive component of deterrence; using defensive measures to disrupt an attack and prevent it from succeeding as well as ensuring that the desired effect is not attained even if defenses are breached.[9] In general, deterrence by denial makes the attack less attractive or less successful from a cost-benefit calculation by prolonging the engagement and/or utilizing more resources.

Prior to the nuclear area (i.e., conventional warfare context), denial was frequently used to achieve extended deterrence due to the alliances and sharing of military and political interests).[10] The primary objective of deterrence by denial is not to defeat entirely but to make it more difficult and expensive for the adversary to succeed in the goal, in other words to disrupt the adversaries cost/benefit balance and deny a rapid victory. Mearsheimer and Gerson argue that deterrence by denial is the primary mechanism for deterrence in conventional conflicts, and that deterrence is more likely "when the attacker believes that his only alternative is protracted war."[11] Similarly, Gerson argues:[12]

> *Conventional deterrence is primarily based on deterrence by denial, the ability to prevent an adversary from achieving its objectives through conflict. If states typically seek short and low-cost conflicts, then conventional deterrence largely depends on convincing an adversary that it cannot achieve its objectives rapidly or efficiently. In this context, the deterrent effect is achieved in large part by the possibility of getting bogged down in a long and costly war of attrition.*

Deterrence by denial has an important advantage over other forms of deterrence (e.g., by punishment) in that it controls escalation;[13] however, deterrence strategies should combine "by punishment" and "by denial". When thinking about deterrence by denial in the conventional weapons context, this strategy is best applied in situations when the stakes are less than existential and military capabilities are credible.[14] Historically, and as we look towards the cyber deterrence paradigm, denial strategies are implemented proportionally to the threats they are intended to deter.

Deterrence by denial must facilitate belief in the adversary(s) of a credible capability. A similar, interchangeable term for deterrence by denial is also used: "dissuasion by denial"[15] which is defined

---

[9] McKenzie, Thomas. (Air Force Research Institute/Air University) "Is Cyber Deterrence Possible?" (Jan 2017) https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

[10] Mitchell, A. Wess. "The Case for Deterrence by Denial" (Aug 12, 2015). https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/

[11] Mearsheimer, John J. (1983) Cornell University Press. "Conventional Deterrence" https://www.jstor.org/stable/10.7591/j.ctt1rv61v2

[12] Gerson, Michael. (2009) Army War College. "Conventional Deterrence in the Second Nuclear Age" https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf

[13] Ibid.

[14] Wirtz, James. "How Does Nuclear Deterrence Differ from Conventional Deterrence?" (Strategic Studies Quarterly, Winter 2018) https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Wirtz.pdf

[15] Davis, Paul. (RAND, Jan 2014) "Toward Theory for Dissuasion (or Deterrence) by Denial"

as "deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate action." Davis states that denial capability does not need to be perfect but is dependent on how the adversary assesses and applies it based on their own level of risk aversion or risk tolerance.

Additionally, much has been written about the potential utility of deterrence by denial to deter even the most highly motivated actors.[16] For example, even terrorists seek to minimize operational risk, and therefore may be deterred by the prospect of being apprehended or killed before completing their attack.[17] Terrorists "may be willing to give their lives, but not in futile attacks," note Davis and Jenkins.[18] The dynamics of cyber conflict are consistent with this perspective. Once vulnerabilities are discovered, they can be patched. The ability to manipulate cyberspace in favor of the defender makes it difficult for attackers to obtain the full potential payoff, yielding the advantage to the defender.[19] Thus, attackers may go to great lengths to ensure their tools are not discovered without some benefit, and this provides the defender with opportunities to create perceptions of operational risk and uncertainty. If by the prospect of resilience, the defender can raise the uncertainty of a fast and easy victory, then the attacker may choose alternative ways and means to achieve their ends, and this is deterrence.

This historical view of deterrence by denial demonstrates that resilience definitions and concepts have always been a part of deterrence. This paper attempts to more clearly demonstrate the connection between cyber deterrence (particularly by denial) and resiliency.

3. ROLE OF CYBER RESILIENCE IN DETERRENCE

The Cyber Deterrence and Resilience Strategic Initiative (CDRSI) at SNL defines resilience as having systems in place that minimize the consequences or impact of an attack, that sustain operations throughout and after an attack, and that recover and adapt to new conditions after an attack has occurred. If an attacker believes that a potential target is resilient in these ways, they face the prospect of fewer gains from attacking that target and would thus probably need to expend more resources to achieve the desired effect than would be required absent such resilience. All else being equal, a calculating attacker would probably choose to target a relatively less resilient system. Cyber resilience complements cyber security to create a comprehensive risk management strategy. The goal of resilience is to survive and overcome to execute the mission which is accomplished by preparing, withstanding, adapting, absorbing, and recovering from an attack.

Deterrence taxonomies abound. We have chosen a taxonomy based on the stage of attack during which costs are imposed or benefits denied. In this frame, deterrence can occur by three mechanisms, including by generating the prospect of resistance, of retribution, and of resilience (the 3Rs). Resistance and resilience often contain common or overlapping tactical implementations. The difference is when the capability affects the attacker in the timeline; resistance occurs prior to or during an attack, and resilience is demonstrated after the attack in how well the affected system can withstand or recover. Resilient systems may have an inherent capability to deter an attacker from deciding to attack or affect the success of their attack but will also have resiliency that will enable

---

https://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf

[16] Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy* 31, no. 1 (2010)

[17] Robert W. Anthony, *Deterrence and the 9-11 Terrorists*, Institute for Defense Analyses (Alexandria, VA, 2003)

[18] Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda* (RAND National Defense Research Institute, 2002), https://www.rand.org/pubs/monograph_reports/MR1619.html

[19] Brantley, "The Cyber Deterrence Problem."

recovery. It is important to note that once the attacker actually *experiences* costs or denial, we have ventured from the realm of deterrence into the realm of actual defense, warfighting, or recovery.

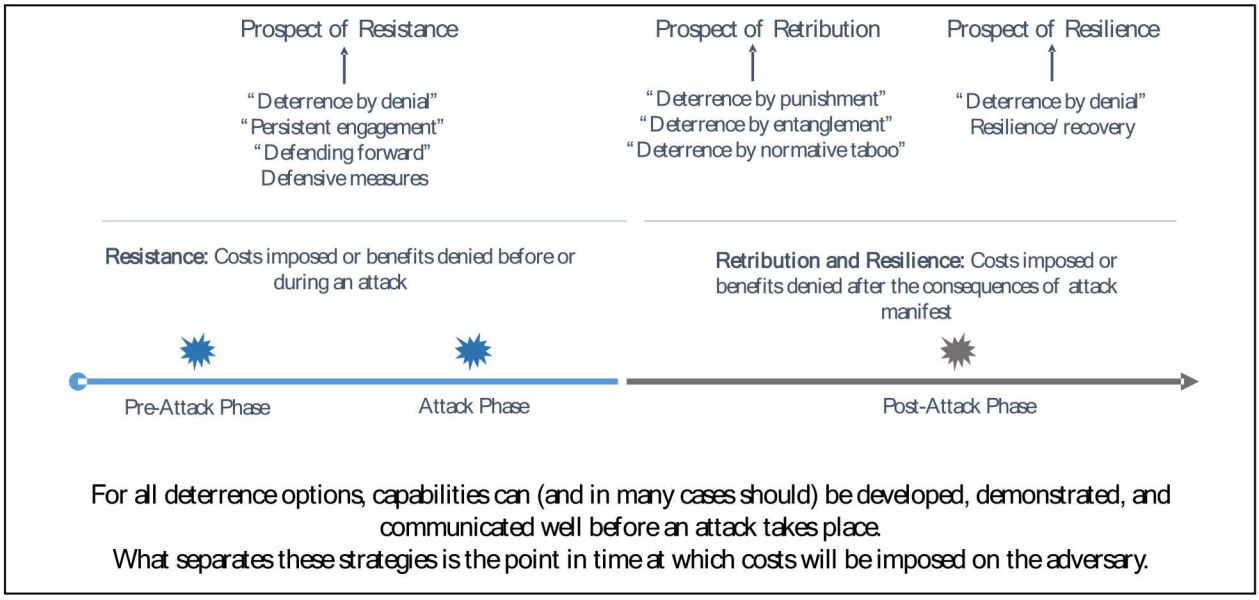

Figure 2. Breakdown of various deterrence mechanisms by time of cost imposition or denial of benefits relative to the attack phase[2]

Just as for more traditional concepts of deterrence by punishment, deterrence by resilience must meet basic criteria for influencing the perceptions of prospective adversaries. Deterrence by the prospect of resilience involves a defender threatening to impose costs and deny benefits to an attacker. (Figure 2) An attacker must perceive these threats as adequately communicated and credible; they must perceive that the defender is capable of conducting and sustaining this added cost imposition, they must be calculating their perceived changes in cost and benefit, even in a rudimentary way, and able to adjust their actions according to these changes. Without these four criteria being met (the "4C's"), resilience measures will fail to deter, that is, influence potential attackers not to attack in the first place, although they may still fulfill the primary function of being a resilient system.

The 4C's that pertain specifically to deterrence through resilience are shown in Figure 3 (see also full table of Deterrence Requirements for Types of Deterrence Strategies in Appendix A):

Communicated	The attacker has previously observed the defender demonstrate that the effects of similar attacks have been mitigated or that the defender has been able to recover promptly.
Credible	Attacker perceives that the defender believes resilience measures are in its own best interest to create and implement (e.g., not too expensive), also that the resilience measures are consistent with the defender's principles (e.g., do not violate certain rights/freedoms).
Capable	Attacker has sufficient visibility into the defender's resilience to believe their attack would be ineffective as well as that it would require too many resources to overcome the defender's resilience measures. The attacker believes the defender has the ability to sustain resiliency across all relevant systems.

Communicated	The attacker has previously observed the defender demonstrate that the effects of similar attacks have been mitigated or that the defender has been able to recover promptly.
Calculated	Attacker perceives that the defender believes the attacker is a rational actor and has sufficient information about the attacker's interest to influence decisions.

Figure 3. The 4 C's of Deterrence through Resilience

3.1. Unique Cyber Domain Challenges and Deterrence through Resiliency

Cyberspace (cyber warfare) is the next significant technological revolution since nuclear weapons and requires strategic thinking around deterrence. There are parallels to conventional deterrence by denial (discussed above) that can be applied to cyber. However, there is not yet a perfect cyber deterrence strategy; in fact, some experts question whether cyber deterrence is possible.[20] The cyber domain has a number of unique challenges such as a wide range of attacker capabilities and adversity to risk, difficulty with attribution, and the inherent overlap between military and civilian functions. Table 1 illustrates the case that there is a role for deterrence by denial in the cyber domain and this is often achieved through resiliency.

Table 1. Deterrence by Denial in the Cyber Domain

Unique Cyber Domain Challenge	Role of Deterrence/Resilience
• Wide range of attacker capabilities, cost/benefit structures, and level of risk adversity.	• Implementing and constantly evolving the environment leads to the principle motive of denial which is to make it more difficult and/or require more resources to achieve the goal • The ability to manipulate cyberspace in the favor of the defender makes it difficult for the attackers to obtain the full potential payoff; few other applications favor the defender as cyberspace deterrence does.[21]
• Attribution is difficult because of the wide range of potential threat actors as well as the use of third-party and proxy to disguise attack origins.	• An unknown attacker may be deterred by denial; building cyber resilience through passive denial defenses (e.g. hardening systems) may make the attack less attractive even if identity is not fully known.[22] • Ensuring a well-protected target and/or the ability to recover quickly (via redundancy and resiliency) influences the cost/benefit ratio, regardless of the ability to attribute (Nye, 2011).
• Cyberspace is a unique operational domain where military	• Deterrence must apply to both virtual and physical aspects of the domain. • Denial tactics that build defensive stability in the environment

[20] Reference Fischerkeller, Michael P. and Harknett, Richard J. "Deterrence is Not a Credible Strategy for Cyberspace," Orbis, Vol. 61, Issue 3, 2017, 381-393

[21] Brantly, Aaron F. (2018 NATO, Virginia Polytechnic and State University) "The Cyber Deterrence Problem" https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf *International Conference on Cyber Conflict*

[22] Nye, Joseph S. "Deterrence in Cyberspace" (June 3, 2019) https://www.project-syndicate.org/commentary/deterrence-in-cyberspace-persistent-engagement-by-joseph-s-nye-2019-06

Unique Cyber Domain Challenge	Role of Deterrence/Resilience
operations cannot be separated from civilian functions (i.e., business, criminal, social).[23]	may be an effective deterrence strategy that avoids disproportionately affecting legitimate, non-military operations in cyberspace. • Retaliation and escalation tactics do not work well in cyberspace; however, denial strategies (i.e., demonstrating resilient systems) can be effective by influencing adversary decisions and mode of operation.[24]

While there are many actions that can be taken to enhance cyber resilience, one example is network segmentation which can create the prospect of resilience. That is, an attack deployed on a segmented network will not spread as easily to other elements of the network, which will continue to operate normally, such that the intended effects are not as broadly distributed as the attacker originally intended. This example highlights building defensive capability and resilience to withstand attacks as well as aligning with the deterrence by denial strategy of insufficient benefits for the attacker.

4. CONNECTIONS BETWEEN DETERRENCE AND RESILIENCE IN CURRENT STRATEGY DOCUMENTS

In the past 5-10 years, there has been increasing strategic discussion regarding cyber resilience as one component of a larger strategy to combat cyberattacks. Numerous organizations, communities, and experts have released strategies and thought pieces around cyber deterrence and resilience such as the Department of Defense (DoD), U.S. Air Force (USAF), U.S. Cyber Command (USCYBERCOM), DHS, and the Cyberspace Solarium Commission, amongst others.

The relationship between resilience and deterrence is particularly important when considering cyber strategy; resilience is an outsized component to a deterrence strategy as compared to past conflict types (e.g., nuclear deterrence). Building cyber resilience into systems strengthens capability for the defender, while at the same time it serves as a deterrent to attackers by hardening the systems to make them too difficult or costly to attack. Several recent reports are highlighted below to demonstrate this new cyber deterrence/resilience paradigm.

- The **DOD Defense Science Board (DSB) Task Force on Cyber Deterrence** published a report in February 2017.[1] The report emphasizes that resilient cyber systems are essential for enabling deterrence at all levels of conflict; that without resilient cyber systems (i.e., for military and critical infrastructure on which military depends) the credibility of deterrence at all levels is weakened. The U.S. must be able to credibly threaten to impose unacceptable costs to even the most sophisticated large-scale cyberattacks. The report included specific recommendations to government agencies and private sector partners to establish and implement a cyber security program to drive sustained improvements in cyber resiliency.

[23] Bebber, Lt. Commander Robert "Jake". (*The Cipher* Brief, April 1, 2018) https://www.thecipherbrief.com/column_article/no-thing-cyber-deterrence-please-stop

[24] Miller, James N. and Neal A. Pollard. "Persistent Engagement, Agreed Competition, and Deterrence in Cyberspace" (*Lawfare*, April 30, 2019). https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace

- The **USAF Cyber Resiliency Office for Weapons Systems (CROWS)**[25] was created in 2017 to develop and standardize a methodology to assess cyber resiliency of weapon systems and integrate activities to ensure that weapon systems maintain mission-effective capabilities despite cyber adversaries.

- The **U.S. Cyberspace Solarium Commission** published a report in March 2020[26] that advocates a layered cyber deterrence approach which includes shaping behavior, denying benefits, imposing costs; these three deterrent layers are supported by six policy pillars. The layered approach prioritizes deterrence by denial specifically by increasing the defense and security of cyberspace through resilience and public- and private-sector collaboration. The report defines resilience as "the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior".

5. CONCLUSION: CYBER RESILIENCE AS A DETERRENT

Without resilient systems, the credibility of deterrence fails. However, without deterrence, resilience still has intrinsic value. We do not need to deter in order to reap the benefits of a society and infrastructure resilient to cyber threats. However, resilience may contribute to deterrence inherently, whether we intend it to or not, and so there are benefits to learning how to maximize the value of resiliency for cyber deterrence strategies. Clarke and Knake[27] adopt paradigms of resilience from social psychology, where "resilience is not about returning to a previous state after an individual experiences trauma, but about adapting to that trauma." This concept of resilience includes the idea that resilient people (and systems) can grow and become stronger after a disruptive or destructive event. While this is a psycho-social example, with deterrence in mind the ability to demonstrate resiliency by withstanding or quickly recovering from a disruption can signal that the cyber system is too difficult or costly to pursue attacking. Similarly, improving after an adverse event can be communicated (e.g., the money and resources dedicated) that can effectively change the cost-benefit calculation for potential attackers.

This paper provides historical and current examples of how resilience and deterrence overlap, particularly in the cyber domain. It is recommended that discussion and progress towards better integration of deterrence and resilience across the government and private sector partners continue (to include collection of metrics to determine the success/failure of different concepts). This is a relatively new theory but further exploration into how resilience can be leveraged for deterrent purposes is essential to cyberspace defense strategies.

[25] https://www.afcea.org/content/cyber-resiliency-feather-crows-flight-cap

[26] "United States of America Cyberspace Solarium Commission", March 2020; https://www.solarium.gov/report

[27] Richard A. Clarke and Robert K. Knake, The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats (New York, NY: Penguin Press, 2019)

APPENDIX A. DETERRENCE REQUIREMENTS FOR VARIOUS TYPES OF DETERRENCE STRATEGIES[2]

	Communicated	Credible		Capable		Calculated
		Rational	Principled	Executable	Painful/Costly	
Resistance	Norms: "XYZ values are an inherent part of who you are. Taking this action violates your core identity." Self-deterrence	The antagonist* perceives that holding these norms and being aligned with a like-minded COA is in their own best interests. (COA = community of actors)	The antagonist believes that these norms are fundamental to their identity and values.	The antagonist believes that taking the proscribed action incontrovertibly and undeniably violates the norms they hold dear.	The antagonist believes that taking the proscribed action is not worth losing their inherent sense of self.	"The antagonist perceives that the protagonist believes that the antagonist is a rational actor, and that given enough information about the antagonist's interests, thresholds, and red lines, the protagonist can influence the antagonist's decisions.
	Persistent engagement: "The protagonist** has ramped up an effort to engage with the antagonist before they reach the protagonist's network, to generate tactical friction and force the antagonist to focus on defense instead of offense."	The antagonist perceives that the protagonist believes that persistent engagement is in the protagonist's best interests, that it is not too expensive and that it will not provoke escalation or retaliation.	The antagonist perceives that the protagonist believes persistent engagement with cyber adversaries is aligned with the protagonist's values and principles.	The antagonist perceives that the protagonist is able to engage with the antagonist persistently (technical capability)	The antagonist perceives that persistent engagement by the protagonist within or around the antagonist's networks will raise the antagonist's operational costs to unacceptable levels	
	Defense: "The protagonist has implemented sufficient measures to diminish the likelihood that the antagonist's attack will achieve the desired effect."	The antagonist perceives that the protagonist believes resistance measures are in its own best interests to create and implement (e.g. not too expensive).	The antagonist perceives that the protagonist believes resistance measures are in line with the protagonist's principles (e.g. do not violate certain rights or freedoms of citizens).	The antagonist has sufficient visibility into the protagonist's security to believe their attack would be ineffective. The antagonist believes that the protagonist's resistance measures are as consistent and effective as the protagonist claims.	The antagonist believes it would require too many resources to overcome the protagonist's resistance measures.	
Retribution	Punishment: Overt threat or precedent: "If the antagonist does X, the protagonist will respond with Y, which will impose unacceptable costs on the antagonist."	The antagonist perceives that the protagonist believes it is in its own best interests to carry out punishment.	The antagonist perceives that the protagonist believes the retributive action is consistent with the protagonist's principles.	The antagonist believes that the protagonist can carry out the retributive action.	The antagonist believes the impacts of punishment would be unacceptably painful.	
	Entanglement: "The economies/ infrastructure/allies/etc. of the antagonist and protagonist are interdependent. Therefore, any action the antagonist takes against the protagonist may also impact the antagonist."	The antagonist believes that they are interdependent with the protagonist. The antagonist believes that the protagonist would allow/tolerate these interdependencies based on the protagonist's own best interests, or that they are unavoidable.	The antagonist believes that the protagonist would allow/tolerate these interdependencies based on the protagonist's principles or values, or that they are unavoidable.	The antagonist perceives that they are in fact interdependent with the protagonist in the way the protagonist claims.	The antagonist believes blowback/shared impacts of attack would be unacceptable.	
	Norms: "The global standard is XYZ. Violating this norm has unacceptable consequences." (COA = community of actors)	The antagonist perceives that the protagonist or COA believe that the norm is important to uphold for their own benefit/livelihood.	The antagonist perceives that the protagonist or COA believe that norm is consistent with their values and principles.	If attributed, the protagonist or COA can impose reputation costs on the antagonist.	Reputation damage will result in unacceptable financial, social, or political costs for the antagonist.	
Resilience	"The protagonist has previously demonstrated that the effects of the antagonist's attacks have been mitigated, or that they (the protagonist) have been able to recover promptly."	The antagonist perceives that the protagonist believes resilience measures are in its own best interests to create and implement (e.g. not too expensive).	The antagonist perceives that the protagonist believes resilience measures are consistent with the protagonist's principles (e.g. do not violate certain rights or freedoms of citizens).	The antagonist has sufficient visibility into the protagonist's resilience to believe their attack would be ineffective. The antagonist believes that the protagonist's resilience measures are as consistent and effective as the protagonist claims.	The antagonist believes it would require too many resources to overcome the protagonist's resilience measures.	

*Antagonist in this table refers to the attacker as used throughout the rest of the document

**Protagonist in this table refers to the defender as used throughout the rest of this document

This page left blank

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Nerayo Teclemariam	08700	nptecle@sandia.gov
Katherine Jones	08721	kajones@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.