5-2023

Integrated Deterrence and Cyberspace: Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest

Joseph L. Billingsley

Heidi K. Kerg , USN

Jim Q. Chen
College of Information and Cyberspace, National Defense University

Michael Navicky

Benjamin Tkach

See next page for additional authors

Authors
Joseph L. Billingsley; Heidi K. Kerg , USN; Jim Q. Chen; Michael Navicky; Benjamin Tkach; and J.D. Work

Integrated Deterrence and Cyberspace

Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest

Edited by Joseph L. Billingsley

College of Information and Cyberspace

The mission of the College of Information and Cyberspace at National Defense University is to educate joint warfighters, national security leaders, and the cyber workforce on the cyber domain and information environment to lead, advise, and advance national and global security.

U.S. Cyber Command

The Commander of U.S. Cyber Command has the mission to direct, synchronize, and coordinate cyberspace planning and operations—to defend and advance national interests—in collaboration with domestic and international partners.

Integrated Deterrence and Cyberspace

Integrated Deterrence and Cyberspace

Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest

Edited by Joseph L. Billingsley

National Defense University Press
Washington, D.C.
May 2023

Cover: General Paul M. Nakasone, USA, Commander of U.S. Cyber Command, delivering opening remarks at the Cyber Symposium on Integrated Deterrence at Fort Lesley J. McNair in Washington, DC, on November 17, 2022.

First printing, May 2023

Contents

In memory of Dr. Roxanne Everetts and Dr. Scott Dade for their commitment to education, the cyber workforce, and the United States.

Acknowledgments

In addition to the essay authors who have shared their intellectual talents for our benefit, there are many individuals and organizations that have contributed to the completion of this publication. Some are listed here.

First is the National Defense University Press team for their expert guidance: Colonel William T. Eliason, USAF (Ret.), Jeffrey D. Smotherman, Joanna E. Seich, John J. Church, and Caroline Schweiter. Next are colleagues at the College of Information and Cyberspace for their endless supply of inspiration, namely Gwyneth Sutherlin, Stuart Archer, Joseph Schafer, and Frank Nuño. The chancellor, Cassandra C. Lewis, deserves special recognition for prioritizing an ever-strengthening relationship with U.S. Cyber Command (USCYBERCOM) to facilitate the success of her students and Nation.

Much appreciation is due to the teammates from USCYBERCOM who selected the essays in this volume—Emily O. Goldman, Michael S. Warner, David R. Swain, Lieutenant Colonel Robert J. Reidel, USA, and Rear Admiral Heidi K. Berg, USN—as well as to John N. Garner for shepherding that process. Finally, thanks to Colonel John M. Gondol, USAF, Colonel Raul Rodriguez-Medellin, USA, and Colonel Scott A. Nelson, USA (Ret.), for strengthening USCYBERCOM's academic engagements with the support of wise leaders including David E. Frederick, Holly M. Baroody, and General Paul M. Nakasone, USA.

Preface

This edited volume represents an important contribution to our thinking on cyberspace and national security. It also serves as one example of an enduring and fruitful relationship between the U.S. Cyber Command (USCYBERCOM) and the College of Information and Cyberspace (CIC) at the National Defense University (NDU).

Essays were solicited in mid-2022 from across the USCYBERCOM Academic Engagement Network, a newly minted body developed in consultation with CIC. The top three submissions were selected by an esteemed committee that included Emily Goldman and Michael Warner. After approval by the USCYBERCOM J5, Rear Admiral Heidi Berg, USN, the authors of the selected essays were invited as panelists at the Cyber Symposium on Integrated Deterrence, an event co-hosted by USCYBERCOM and CIC at NDU, located at Fort Lesley J. McNair in Washington, DC, on November 17, 2022.

The photograph on the cover of this volume captures General Paul M. Nakasone, USA, commander of USCYBERCOM, providing the opening remarks for the November event. In those remarks, General Nakasone referred to CIC as "our college" in recognition of the close collaboration between the functional combatant command he currently leads and the hosting war college–level institution aligned to its mission area.

In the National Defense Authorization Act for Fiscal Year 2017, Congress renamed the NDU Information Resources Management College as CIC to prioritize the strategically oriented educational needs of the growing Defense Cyber Workforce. Less than a year after the renaming ceremony, the team at CIC hosted the 2018 Cyberspace Strategy Symposium. The central question of that 2018 event was "What are the foundational organizing principles we need to operate more effectively in cyberspace?" One such principle that event helped to develop was that of *persistent engagement*, which has since gained wide popularity. That event was the first in a series of USCYBERCOM strategy symposia supported by CIC, the most recent of which was the November 2022 event that this volume is primarily associated with.

The concepts shared herein may help with a better understanding of the current state of cyberspace and national security and how we may shape their future(s). For the reader who may be a strategist, researcher, or practitioner focused on this ever-evolving intersection of competing priorities, I trust you will glean many important strategic insights.

—Joseph L. Billingsley,
Editor

Introduction

By Heidi Berg

The 2022 National Defense Strategy (NDS) revolves around the concept of integrated deterrence. It calls for seamless operations across domains, theaters, and the spectrum of conflict, leveraging nonmilitary tools, buttressed by partners and supported by network integration. The NDS explains that while the joint force seeks to deter aggression, it is also campaigning to counter adversary moves short of armed conflict and building enduring advantages to sustain military strength that convinces adversaries that they cannot achieve their aims through armed conflict. Integrated deterrence is based on the recognition that our adversaries have holistic strategies and that the United States requires its own holistic approach to secure American interests and advance national goals. Accordingly, it strives to optimize the use of all instruments of national power.

This collection of essays adds to the ongoing operational and academic discussion on how integrated deterrence—one of the three overarching NDS strategies, which also include campaigning and building enduring advantage—supports national interests. It should also assist U.S. Cyber Command in navigating the roles of cyberspace operations in competition, crisis, and

conflict in support of the new NDS's priorities: to defend the homeland, deter aggression, deter strategic attack, and build a resilient joint force.

This edited volume begins with Jim Chen's "Deterrence in Cyberspace: An Essential Component in Integrated Deterrence," which proposes that deterrence is an important means in preventing war and maintaining stability. Chen examines the essence of deterrence and recognizes that different types of deterrence are suitable for different types of strategic contexts. The effectiveness of one type of deterrence is determined by its specific strategic context. To enable the dynamics, Chen proposes a multilevel and multi-aspect deterrence architecture for the integrated deterrence strategy. This architecture contains the spectrum of the strategic environments both below and above the threshold of armed conflict; the dimension of varied instruments of national power, such as diplomatic, information, military, economic, and law enforcement; and alliances and partnerships.

The second essay, "Cross-Domain Cyber Incidents and State Responses," by Michael Navicky and Benjamin Tkach, postulates that creating cyber deterrence requires analysis of cyber deterrence across and within the multi-domain threat environment. The authors argue against the persistent assumption that engagement in the cyber realm is a low-cost endeavor. For the types of cyber activity that the United States seeks to deter, adversaries' sunk costs are substantial, in both personnel and infrastructure. Cyber deterrence efficacy is too often quantified by acts of cyber attacks that, while numerically substantial, are more akin to international freedom of navigation or airspace violations. The authors posit that in the absence of norms necessary to categorize violations, the Department of Defense must develop a typology for cross-domain cyber-capability deterrence signaling.

The volume concludes with J.D. Work's "Cumulative Outcomes of Counter–Cyber Operations Campaigns: Contributions to Integrated Deterrence," which considers newly promulgated concepts of integrated deterrence, which once again raise questions of how cyber operations contribute to foundational U.S. defense strategies. Although doctrines advanced on the underpinnings of cyber persistence theory continue to offer strong explana-

tory value for interactions in and through the domain, decisionmakers still seek to understand how to reconcile these new ideas with long-standing objectives across U.S. posture. Work reinterprets that causal mechanisms by the opposition may discount relative benefits from aggression relative to restraint, given the erosion of their capabilities and diminution of their options, the cumulative outcome of counter–cyber operations campaigns.

There is no competition, crisis, or conflict in the 21st century that will occur without some cyber element. We live in a digital age, in which rival powers affect one another through cyber operations before, during, and after any kinetic clash. Strategic competitors present an array of challenges to the United States, undermining the Nation's strengths by exploiting its cyber vulnerabilities. They also engage in various forms of malign behavior, coercion, and aggression below the threshold of armed conflict. Cyberspace is a major arena in this strategic competition; the terrain is rich with poorly defended resources, and adversaries' campaigns of theft, disruption, and disinformation have produced strategic gains without the risks that accompany the use of force.

My hope is that this collection of essays can further advance our understanding and implementation of national strategy in support of our national interests. Effective military power cannot be exercised and employed without cyberspace support. Cyber capabilities, forces, and operations are essential to integrated deterrence and our ability to win in competition. Cyberspace will be vigorously contested as adversaries strive to leverage and manipulate information in competition; we must shape conditions to enable the joint force's success in crisis and conflict. The United States cannot afford to cede initiative in competition, crisis, or conflict, especially in and through cyberspace. We must find a way to challenge adversaries even as they enjoy fewer government or societal constraints, are more willing to accept risk, and have been actively campaigning for many years.

1

Deterrence in Cyberspace: An Essential Component in Integrated Deterrence

By Jim Q. Chen

Deterrence is an important means to prevent war and maintain stability. It is usually expected to be applicable in all military domains: land, sea, air, space, and cyberspace. It is defined in Joint Publication 3-0, *Joint Operations*, as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[1]

The importance of deterrence in national security is clearly stated by multiple authors, including Herman Kahn, Thomas Schelling, and Keith Payne.[2] Kahn's work lays the foundation for the deterrence-by-denial strategy, whereas Schelling's work lays the foundation for deterrence by punishment. These two strategies, focused on nuclear deterrence, have shaped the current strategies regarding strategic stability.

However, in a virtual environment, deterrence seems to lose its sharp edge, at least currently. Richard Harknett and Max Smeets discuss why cyber deterrence fails and why it must be fixed.[3] To account for this phenomenon, some scholars have started to question the existence of deterrence in cyberspace and advocate for resorting to other means to support some function-

alities needed for cyber operations. Nevertheless, other scholars insist on the pursuit of deterrence in cyberspace because the crucial role of deterrence is not replaceable in their view. Martin C. Libicki argues for cyber deterrence.[4] In addition, he shows the differences among cyber deterrence, nuclear deterrence, and criminal deterrence. Both schools of thought have made some valid points in their arguments. However, a solution that can be accepted by both sides is hardly to be reached if other aspects and instruments of national power are not considered.

This chapter intends to establish a novel solution. First, it examines the essence of deterrence. Second, based on analysis of the various strategic contexts, it recognizes the fact that different types of deterrence are suitable for different types of strategic contexts. It argues that the effectiveness of one type of deterrence is determined by the specific strategic context that it belongs to. Third, based on this argument and the requirements of the 2022 National Security Strategy (NSS) and the 2022 National Defense Strategy (NDS), it proposes an innovative multilevel and multi-aspect architecture for the integrated deterrence strategy. This architecture encompasses the levels of severity both below and above the threshold of armed conflict as well as the aspects/scopes of varied instruments of national power, such as diplomacy, information, military, economy, law enforcement, alliances, and partnership. Fourth, it explores the unique role that deterrence plays in cyberspace given this multilevel and multi-aspect deterrent architecture. It argues that deterrence is absolutely needed in cyberspace for strategic reasons and examines various ways of conducting deterrence in cyberspace, especially ways that resort to strategic surprise. It shows that a thorough understanding of cyberspace's strategic context helps the design and development of innovative cyber deterrent capabilities. These capabilities will be efficient and effective in the strategic contexts they belong to. Fifth, it discusses the benefits of the multilevel and multi-aspect architecture for the integrated deterrence strategy.

This novel approach has several benefits. With the help of strategic context for cyberspace, it can seamlessly link the role of cyberspace operations, both defensive and offensive, to the NDS concept of integrated deterrence.

Given the architecture for integrated deterrence, various strategic contexts are holistically integrated within one system. Should one strategic context be changed to another, the change to a relevant deterrence type can be easily made. Moreover, this architecture helps decisionmakers and strategists consider the overall picture of national security when they are facing challenges seemingly coming from one domain or aspect. In addition, this approach will help to create new deterrent capabilities for various strategic contexts.

Ultimately, research shows that deterrence in cyberspace is an essential component of integrated deterrence. This novel approach can certainly enrich integrated deterrence as more domains and aspects are added into the strategy, thus making it more powerful and more flexible.

Essence of Deterrence

To understand the essence of deterrence, one needs to have a better understanding of its goal, which is to force deterrent targets (namely, people who are going to be deterred) to give up their current aggressive commitment or at least restrain their behavior. In other words, the goal of this strategy is to change the decisionmaking calculus of deterrent targets. When they see no significant gains but only high costs in their commitment, they are more likely to discontinue their current engagement. Robert Art and Kelly Greenhill describe how coercion can lead to a change in an opponent's behavior.[5] Bernard Brodie holds that atomic weapons are made not for use but to keep the opponents from using them.[6] These situations clearly show successful deterrence.

Note that, in general, deterrent targets are hard to convince unless they are overwhelmed with fear and anxiety. Only when these targets see no chance of changing the upcoming results and the unavoidable consequences that threaten their survival and/or reputation will they start to think of compliance with what they are forced to do. In this sense, deterrence works in the human mind.

To make deterrence work, the following two questions must be asked:

- How can such a psychological state be created?
- What special deterrent capabilities can be used?

To address the first question, both the dominant way and the emerging way of creating such a psychological state should be considered.

For a long time, such a psychological state has been created via physical forces with current technological superiority. Potential physical punishment can fully convince deterrent targets that they have no chance of achieving their goal and their fate is doomed if they do not stop what they are committed to.

Since the creation of the virtual world, in the late 20th century, another option has emerged. This option makes it possible to create such a psychological state via digital or virtual means. Unfortunately, not much research is devoted to this study currently; further research needs to be conducted.

To address the second question, both existing and potential capabilities should be considered.

To create a psychological state by physical means requires weapons with technological superiority. Nuclear weapons serve as an example; they are chosen because they can cause tremendous casualty and destruction to adversaries. The consequences of being attacked via these weapons are totally beyond what adversaries can bear in any circumstances. The destruction is absolute. Because the use of these weapons would have such a serious impact, it is restricted, considered a last resort. If both sides possess these weapons and neither side ventures to use them first, a balance is created.

Currently, the notion of deterrence is heavily influenced by nuclear deterrence strategies, which make use of nuclear weapons' paramount threatening capability. But the notion of deterrence does not exclude other ways of generating deterrent effects, at least theoretically. If there is a capability that can push deterrent targets into an extreme psychological state that induces them to stop or change their behavior, this capability serves as a capability for deterrence. It does not matter whether this capability is physical, digital/

virtual, or a combination of the two. If it can help to achieve the deterrence outcome, it is worth exploration.

Specific capabilities are bound by specific contexts or environments. This means that a capability that works in one context may not be as effective in another.

Context-Based Deterrence Capabilities

Deterrence capabilities will be effective only when they are employed in the contexts they are designed for. Hence, it is critical to understand the varied contexts.

The physical world is characterized by entities, objects, environments, and humans. In conflicts within the physical world, weapons are always used, because what matters is what can be seen, touched, felt, and experienced. Forces and capabilities can be used to generate psychological impact, which can then compel adversaries to stop or change their behavior, thus generating effective deterrence. But the capabilities employed must be superior to those used by adversaries to guarantee effective deterrence. For instance, those who have nuclear weapons possess superiority over those who do not. Likewise, those who have a nuclear triad capability possess superiority over those who have only a land-based nuclear capability.

It is the difference in capabilities that lays the foundation for deterrence. To make deterrence work, this mismatch in capabilities is intentionally made known to adversaries. Messages sent to deterrent targets must be clear and not only demonstrate the capabilities but also the willingness to use them whenever needed in the domains of land, sea, air, and space. Besides, there are various choices of physical weapons at different levels of armed conflicts, which can be escalated or de-escalated. In most cases, physical weapons are mainly used within armed conflicts.

Deterrence in the physical world possesses the following characteristics:

◆ The purpose of deterrence strategies is to prevent further escalation of conflicts and avoid war.

◆ The deterrent capabilities designed, developed, and employed are for armed conflicts. Hence, they are used above the threshold of armed conflict.

◆ The display of capabilities and the demonstration of willingness to use them are transparent and unambiguous.

◆ The entry level is high, because tremendous investment is needed for the education of professionals as well as the design and development of weapons with technological superiority.

◆ The main deterrent sources are physical, the potential destructive impacts indicated are physical and psychological, and the actual deterrent consequences are psychological and physical.

Cyberspace, which is made up of a combination of both the physical world and the virtual, possesses special characteristics that help to shape its strategic environment. To have a better understanding of this strategic environment, we must understand the critical factors of cyberspace as well as the essential capabilities derived from these critical factors.

Data serve as one pillar of cyberspace. The ways they are generated, processed, transmitted, stored, used, and managed help to shape the environment in cyberspace. In the virtual world, electromagnetic signals, invisible to the naked eye, are used for rapid data transmission. This fact makes it possible to be fast and anonymous in cyberspace, and the mathematical foundation built into computers makes it possible to be accurate and precise. As a result, with respect to cyber operations, cyberspace possesses the following critical factors: speed, accuracy, precision, dynamics, and stealth.[7] Having individual operators is another critical factor; any cyber operation depends on operators who manipulate devices, systems, applications, and/or data. The details of capabilities used for deterrence in cyberspace are seldom revealed; the source codes are always kept secret. But the willingness to use them is made known publicly.

As pointed out by General Paul Nakasone, "the locus of struggle for power has shifted toward cyberspace, and from open conflict to competitions

below the level of armed attack."[8] Note that the entry level in cyberspace is low.[9]

Deterrence in the virtual world possesses the following characteristics:

◆ The purpose of deterrence strategies is to stop aggressive cyber operations from deterrent targets and prevent cyber conflicts from further escalating into armed conflicts.

◆ The deterrent capabilities designed, developed, and employed are for both non-armed and armed conflicts. Hence, they are used both below and above the threshold of armed conflict.

◆ The display of capabilities is opaque and ambiguous, whereas the demonstration of willingness to use the capabilities is transparent and unambiguous.

◆ The entry level is relatively low, because the cost of design and development of cyber weapons with technological superiority is relatively low compared with the cost of design and development of nuclear weapons (even though tremendous investment is needed for the education of professionals).

◆ The main deterrent sources are virtual; the potential destructive impacts indicated are virtual, physical, and psychological; and the actual deterrent consequences are psychological, virtual, and physical.

Comparing the characteristics in cyberspace with those in the physical world, we can quickly see that there are differences in the purpose of deterrence, the requirement for deterrent capabilities, the requirement for the display of capabilities, the requirement for the demonstration of willingness to use the capabilities, the requirement for the investment of human resources as well as research and development, deterrent resources, the potential destruction impacts indicated, and the actual deterrent consequences.

Given these differences, it is hard to imagine that the deterrence strategies designed solely for the physical world could be effective in cyberspace. The strategy of deterrence by denial and the strategy of deterrence by punishment are two examples.

The strategy of deterrence by punishment is hard to employ in cyberspace; proportional punishment, immediate responses, and jurisdiction are usual challenges. In almost all cases, the chances of using nuclear responses to cyber breach operations are slim, because they are not at the same level of severity as cyber breach operations; such a response would not be proportional. In some cases, economic sanctions and diplomatic protests are introduced, but such responses are frequently delayed. In other cases, retaliatory cyber operations are launched. Because of the anonymous and hidden nature of some cyber operations and the amount of time needed for attribution, immediate responses are hard to guarantee.

The strategy of deterrence by denial requires strong defense in cyberspace. However, because of the complexity of systems (namely, hidden layers that users do not have access to and/or codes difficult to comprehend by users without technical knowledge) and the opaque nature of the cyber supply chain, adversaries have consistently exploited vulnerabilities within systems, thus defeating layers of defense. Restricted by the amount of time needed for attribution and accurate targeting, retaliation in cyberspace is either delayed or is left aside. As a result, this deterrence strategy does not work in some cases.

As discussed, in cyberspace, the strategy of deterrence by punishment is hard to execute, and deterrence by denial may not be successful in all cases. These strategies are specifically designed for conflicts in the physical world, not cyberspace.; they may or may not be effective in the cyber context.

A Novel Multilevel and Multi-Aspect Architecture for the Integrated Deterrence Strategy

Varied deterrence capabilities are bound by the contexts they are designed for. We may wonder whether these varied deterrence capabilities could be tied together. If the answer is yes, then we may wonder what way they could be tied together to achieve effective deterrence.

Each context possesses its uniqueness. A context in the virtual world is certainly different from a context in the physical world in many aspects.

However, from a strategic perspective, all these contexts are related and must be dealt with comprehensively. Accordingly, varied deterrence capabilities tailored to varied contexts need to be organized holistically. Beyond doubt, integrated deterrence is the way to go to bring all deterrence capabilities together. However, in the current version of the integrated deterrence strategy, it is not clear how the varied deterrence capabilities and varied contexts are tied together. This chapter intends to address this issue by proposing a novel multilevel and multi-aspect architecture for integrated deterrence.

In the 2022 NSS, *integrated deterrence* is defined as "the seamless combination of capabilities to convince potential adversaries that the costs of their hostile activities outweigh their benefits."[10] It entails integration across domains, regions, the spectrum of conflict, the U.S. Government, and allies and partners. In the 2022 NDS Fact Sheet, three primary ways of advancing Department of Defense goals are mentioned: integrated deterrence, campaigning, and building enduring advantages. Regarding integrated deterrence, the fact sheet states:

> *Integrated deterrence entails developing and combining our strengths to maximum effect, by working seamlessly across warfighting domains, theaters, the spectrum of conflict, other instruments of U.S. national power, and our unmatched network of Alliances and partnerships. Integrated deterrence is enabled by combat-credible forces, backstopped by a safe, secure, and effective nuclear deterrent.*[11]

These national strategies clearly list the key components of integrated deterrence, namely, the nuclear deterrent, cross-domain and cross-aspect interagency efforts, and cooperation with alliances and partners.

Clementine G. Starling, Tyson K. Wetzel, and Christian S. Trotti describe the integrated deterrence concept as an expansion from traditional to strategic deterrence by promoting whole-of-government deterrence plus

whole-of-alliance deterrence.[12] Whole-of-government deterrence entails the use of instruments of national power.

The essence of these strategies can be captured by a multilevel and multi-aspect architecture proposed here. Following the model of deterrence levels previously proposed by Jim Chen, this proposed architecture, shown in the figure, consists of a vertical axis that represents the escalation and de-escalation of conflict and a horizontal axis that covers multiple instruments of national power and alliances.[13]

Note that this architecture captures competition and conflicts at various levels of severity, both below and above the threshold of armed conflict. The following levels are below the threshold of armed conflict:

- Level 0 is the level of intelligence-collection operations.
- Level 1 is the level of influence campaigns.
- Level 2 is the level of cyber operations and cyber-enabled information operations.

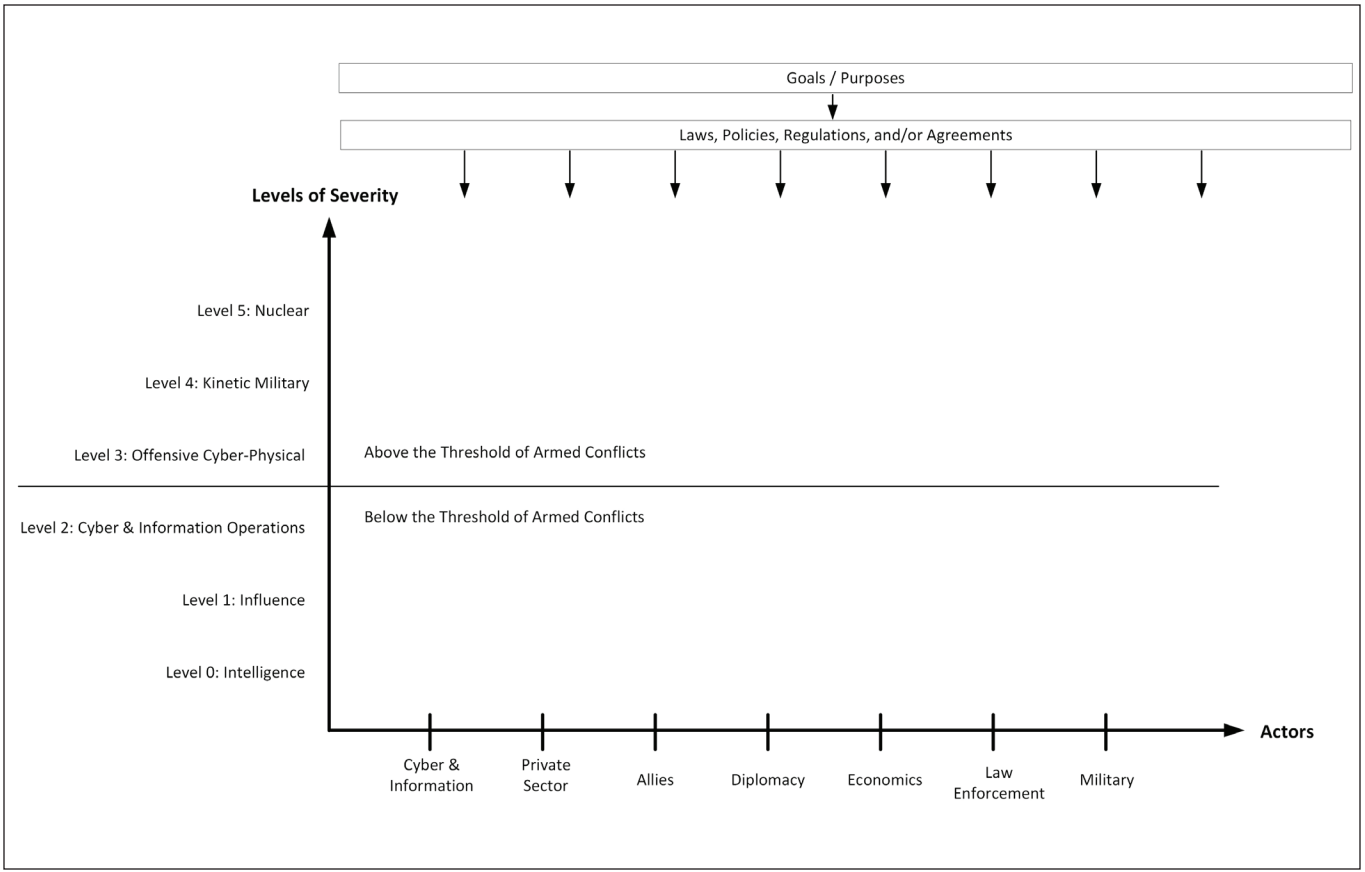
The following levels are above the threshold of armed conflict:

- Level 3 is the level of offensive cyber-physical operations and campaigns.
- Level 4 is the level of kinetic and conventional military campaigns.
- Level 5 is the level of nuclear warfare.

Going from a lower to a higher level indicates an escalation of conflict and an increase in deterrence intensity; going from a higher to a lower level designates a de-escalation of a conflict and a decrease in deterrence intensity.

This architecture also captures the varied elements that can be involved in deterrence endeavors: information, the private sector, allies, diplomacy, economics, law enforcement, and the military. Each has a focus on a certain level or levels. Only the military has access to all levels. Having more elements involved in the execution of deterrence means widening the scope of deterrence; having fewer means narrowing the scope of deterrence.

Figure. Multilevel and Multi-Aspect Architecture for Integrated Deterrence Strategy



The goal of the integrated deterrence strategy is to execute deterrence at an appropriate level for an effective outcome while making use of relevant resources and support from other domains and aspects. The architecture proposed here can help achieve this goal with a platform that supports flexibility in the execution of deterrence in the modern era, wherein the cyber or the virtual world coexists with the physical. Deterrence, if it to be is effective, should be applied to both the cyber and the physical worlds.

Being dynamic and flexible, this architecture makes it possible to have different levels of deterrence in different strategic contexts. For example, that there is no need to execute nuclear deterrence at Level 2, namely, the level of cyber operations and cyber-enabled information operations. However, as a situation escalates, the level of severity may potentially reach Level 5, namely, the level of the nuclear warfare. Nuclear deterrence can be proportionally executed in an appropriate context. The nuclear deterrent is positioned in the integrated deterrence strategy to support all lower-level deterrent measures and serve as the ultimate deterrent. This satisfies the requirement of the 2022 NSS, which states that "nuclear deterrence remains a top priority for the Nation and foundational to integrated deterrence."[14]

Being dynamic and flexible, this architecture also makes it possible to widen the scope of deterrence. Instead of resorting only to the military force of one country, it enables allied forces to get involved on request. By increasing the number of aspects potentially involved, this structure amplifies the weight of deterrence. Similarly, by engaging the private sector at the levels below the threshold of armed conflict, it enables more capabilities to be assembled for executing deterrence in cyberspace.

In this architecture, Level 5 is focused on total physical destruction, whereas Level 2 is focused on surprise, especially surprise from the digital/virtual world.

To summarize, this multilevel and multi-aspect architecture for integrated deterrence strategy can satisfy the requirements of the 2022 NSS and NDS by bringing varied deterrence capabilities and varied strategic contexts together holistically, thus achieving proportional and effective deterrence effects.

Deterrence in Cyberspace

As discussed, deterrence must be proportional and effective at every level. Should there be few or no deterrence capabilities at one level, the integrated deterrence strategy would not be effective. Therefore, deterrence in cyberspace is required to support the overall integrated deterrence.

Without proportional and effective deterrence in cyberspace, the number of cyber attacks would increase, personal information would be taken and misused without permission, intellectual property would be stolen, legitimate election processes would be compromised, and national security would be threatened. Should cyber conflicts at Level 2 escalate to cyber-physical conflicts at Level 3, human casualty and property damage could be expected via attacks against critical infrastructure.

Michael Fischerkeller and Richard Harknett mention two strategic spaces.[15] One is the strategic competitive space short of armed conflict, the other the strategic space of militarized crises and armed conflict. The first space contains a competitive interaction dynamic. The second space encompasses escalation dynamics. The strategic competitive space short of armed conflict is the place where the persistent engagement strategy and the defend-forward strategy are applied, whereas the strategic space of militarized crises and armed conflict is the place where kinetic and even nuclear weapons may be used. Deterrence lies between these two spaces. However, the deterrence space is not discussed in this approach. Hence, this approach is limited. Leaving a blank spot on the continuum is not a good idea, especially with one critical space left unused. Hence, ways of creating deterrence in cyberspace should be explored for strategic reasons.

One level of deterrent is simply not enough; the deterrent will be either too strong or too weak in a non-associated strategic context. For instance, if the nuclear deterrent is chosen as an option for deterrence in cyberspace, it will not be executed as a response in almost all cases, because it is not proportional. Likewise, if a kinetic military campaign is chosen as an option for deterrence in a nuclear war, it will not work, because it is not proportional. It is important to employ context-based deterrence.

As noted, Chen states that cyberspace possesses the following critical factors: speed, accuracy, precision, dynamics, anonymity, stealth, and individual operators.[16] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett mention four important variables in the cyber strategic environment: accessibility, availability, speed, and affordability.[17] Fischerkeller et al. hold that because the cyber strategic environment is "the product of interconnectedness, constant contact, and inherently reconfigurable terrain and capacity to act across and through that domain,"[18] persistence—which is "able to effectively anticipate and persistently set the conditions of security" in one's favor "in and through cyberspace"[19]—is the key for success in cyberspace. Hence, the persistent engagement strategy should be executed in the strategic competitive space short of armed conflict. Even though their analysis is not specifically for deterrence in cyberspace, it is applicable to the strategic context of cyberspace.

Given this specific strategic context, we may ask the following question: What can serve as a context-based deterrent in cyberspace?

To achieve the goal of stopping aggressive cyber operations and preventing cyber conflicts from escalating into armed conflicts, strategic surprise can serve as a context-based deterrent in cyberspace. Strategic surprise can overwhelm deterrent targets with shock, confusion, and fear, at least for a period, making them lose the will to continue their commitment. This period certainly offers deterrent initiators an opportunity for superiority.

Ephraim Kam points out that "surprise is a basic and recurring event in human life. Still, neither the repeated occurrence of surprises nor our assumption that life has surprises in store for us makes us any less vulnerable to its impact."[20] According to Kam, surprise occurs in any or all the following conditions:

- when "an act or development has taken place contrary to our expectations, thus proving our assumptions to be ill founded"
- when an act or development occurs "without warning, catching us unprepared; hence our inadequate response"

◆ when "the sudden happening provokes our emotions, which, when strong enough, may throw us off balance, at least for a while."[21]

How can strategic surprise be created in the minds of adversaries? Following Kam, it can be created when an act or development goes against the expectations of adversaries; catches them unprepared; and provokes shock, confusion, and fear in their minds. To satisfy these conditions, the state of uncertainty is needed. The state of uncertainty, in turn, relies on ambiguity, anonymity, speed, and unique capabilities such as intelligence collection and analysis, precision, accuracy, and stealth maneuver. Chen, and Chen and Alan Dinerman provide some detailed discussion about these capabilities.[22] These are also the critical factors in cyberspace, where they can be employed to create deterrent effects.

Thus, strategic surprise supported by stealth operations is one of the components in the strategy of deterrence by engagement and surprise, as proposed by Chen.[23] This deterrent can perform the functions listed below to overwhelm deterrent targets with fear and anxiety.

First, various types of warning messages can be sent to deterrent targets via unexpected means, to unexpected devices, and at unexpected times. Relevant intelligence collection and analysis can help identify deterrent targets accurately, and relevant information about deterrent targets can help craft precise warning messages. These messages can be quickly sent to devices not directly involved in cyber attack operations by unexpected means at unexpected times, indirectly indicating that the deterrent targets are being closely monitored and their identities are known. The frequency, target locations, message delivery methods, and message transmission times can be changed unpredictably, thus creating uncertainty; leading to shock, confusion, and fear; and creating a deterrent effect.

Second, various indirect surprise cyber operations can be launched against specific deterrent targets without prior notice. Within a short period of time after deterrent targets launch cyber attacks, they will be taken by surprise: on their own devices that have not been used in cyber attack operations, some applications will suddenly stop working or mysteriously disappear; the con-

tents of some files on these devices will be suddenly changed; some files and folders on these devices will be removed. What is more, if deterrent targets have Internet-of-things devices, these devices will mysteriously cease to work or suddenly act strangely. Such events, which catch deterrent targets unprepared, may lead them to think that they have been watched. These events can also provoke shock, confusion, and fear. Overwhelmed by fear supported by uncertainty, these targets can be deterred.

Third, various direct surprise cyber operations can be launched specifically against deterrent targets without prior notice. Specifically, the devices that deterrent targets use for launching attacks, as well as the botnets they compromise and use in attacks, will unexpectedly malfunction, ceasing to accept instructions or getting frozen. In addition, the packets that they send out during cyber attacks will either get dropped in networks or fail to reach their destinations. The network in which an initial cyber attack is launched oddly gets congested, thus making cyber attack operations impossible. All these effects are contrary to the expectation of the deterrent targets, challenging their initial assumptions. Being disabled in cyber attack operations makes deterrent targets wonder what has happened and throws them off balance psychologically. Again, overwhelmed by fear supported by uncertainty, these targets can be deterred.

Fourth, cyber-enabled information operations may be launched against deterrent targets without warning, via unexpected means, to unexpected devices, and at unexpected times. Specifically, once deterrent targets are identified, such operations can be launched to damage their reputation via social media. Being thus thrown off balance, these targets can be overwhelmed by fear supported by uncertainty and, eventually, deterred.

There are other types of surprise operations that can be used effectively as deterrents in cyberspace. All the instances show that surprise, which is capable of provoking shock, confusion, and fear in adversaries' minds, can effectively serve as a deterrent, at least at Level 2 and Level 3. Note that operations at Level 2 are below the threshold of armed conflict. The deterrence at

this level is not as powerful as the deterrence at the level of nuclear weapons; however, it is proportional and serves its purpose.

Deterrence at the offensive cyber-physical level is above the threshold of armed conflict. Here, cyber means are used for military purposes. Critical infrastructure is held hostage in deterrence. A state of uncertainty in targets can be generated with the help of ambiguity, anonymity, speed, and unique capabilities, such as intelligence collection and analysis, precision, accuracy, and stealth maneuver. This type of kinetic military operation or campaign can overwhelm deterrent targets with shock, confusion, and fear. Consequently, a deterrent effect is created, and deterrent targets are deterred.

Cyber capabilities have a relatively short life span compared with the life span of capabilities in the physical world. Thus, building stealth capabilities is a continuous and unavoidable task. Nonetheless, with the help of artificial intelligence, which consists of machine learning and data analytics, this task becomes doable. Because this topic is not the focus of this chapter, the specific methods for creating surprise capabilities by means of artificial intelligence are not discussed here.

Deterrent capabilities in cyberspace can be used either below or above the threshold of armed conflict. The entry level for building cyber-based deterrent capabilities is relatively low, and innovative cyber-based deterrent capabilities should be created continuously, because they have a relatively short life span. Cyber-based deterrent capabilities are applicable not only in cyberspace but also in the physical world. With the proposed multilevel and multi-aspect architecture for integrated deterrence, the differences in deterrent purposes, capabilities, and applications can be explicitly and successfully captured.

Benefits of the Multilevel and Multi-Aspect Architecture for the Integrated Deterrence Strategy

The proposed architecture for the integrated deterrence strategy captures the essence of the 2022 NDS. It successfully reveals the relationships among different components, especially the dependency relationship, and

makes it possible to execute deterrence proportionally and effectively within a certain strategic context, increasing its chance of being successful. This holistic approach also makes deterrence dynamic and flexible, with the ability to resort to varied deterrents in varied strategic contexts. This architecture for integrated deterrence differentiates between strategic contexts below and above the threshold of armed conflict. Recognition of different strategic contexts furthers the development context-based deterrent capabilities and helps make deterrent capabilities efficient and effective within their contexts.

With the introduction of the multilevel and multi-aspect architecture for the integrated deterrence strategy, some challenging questions can be successfully addressed. In this new approach, a deterrent is no longer treated as something that can be executed anywhere. Instead, it must be executed within a relevant strategic context to be effective.

This holistic approach not only makes deterrence in cyberspace a part of the overall integrated deterrence but also provides national security decisionmakers and strategists with ways of executing proportional and effective deterrence at different levels and within different contexts, thus successfully achieving national security goals. Ultimately, the research shows that deterrence in cyberspace is an essential component of integrated deterrence.

This innovative approach can certainly enrich integrated deterrence; more domains, dimensions, and facets can be added, thus making the strategy more powerful and more flexible.

Conclusion

Under the multilevel and multi-aspect architecture for integrated deterrence, varied deterrence capabilities and varied strategic contexts can be holistically tied together, thus making the integrated deterrence strategy more powerful and more flexible.

We cannot go without deterrence in cyberspace because cyberspace is a significant element of national security, and deterrence in cyberspace is an essential component in integrated deterrence. Without deterrence in cyber-

space, which may be applied in gray zone contexts, deterrence will be incomplete. Deterrence in cyberspace will work within its strategic contexts.

The proposed architecture makes it possible to create varied novel deterrent capabilities at different levels and within different aspects, thus enhancing the role of deterrence in national security and in cyberspace.

This holistic approach can not only provide national security decisionmakers and strategists with ways of effectively using all deterrent capabilities at different levels at their disposal to maintain strategic advantage but also make deterrence in cyberspace a part of the overall integrated deterrence. As a result, national security decisionmakers and strategists will be able to execute proportional and effective deterrence based on the requirements of strategic contexts, thus successfully achieving national security goals.

Notes

[1] Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017, Incorporating Change 1, October 22, 2018), GL-8, https://irp.fas.org/doddir/dod/jp3_0.pdf.

[2] Herman Kahn, *The Nature and Feasibility of War and Deterrence*, P-1888-RC (Santa Monica, CA: RAND Corporation, 1960); Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), https://www.rand.org/pubs/papers/P1888.html; Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice From the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008).

[3] Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes: The Other Means," *Journal of Strategic Studies*, Spring 2020, 1–34, https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354.

[4] Martin C. Libicki, *Cyberspace in Peace and War*, 2nd ed. (Annapolis, Maryland: Naval Institute Press, 2021); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[5] Robert J. Art and Kelly M. Greenhill, "Coercion: An Analytical Overview," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (Oxford: Oxford University Press, 2018), 3–32.

[6] Bernard Brodie, ed. *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt Brace, 1946).

[7] Jim Chen, "AI-Based Deterrence in the Cyber Domain," in *Proceedings of the 14th International Conference on Cyber Warfare and Security*, ed. Noëlle van der Waag-Cowling and Louise Leenen (Reading, UK: Academic Conferences and Publishing International, 2019), 38–45.

[8] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019), 11, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.

[9] Paul M. Nakasone, interview by William T. Eliason, *Joint Force Quarterly* 92 (1st Quarter 2019), 4–9, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

[10] *National Security Strategy of the United States of America* (Washington, DC: The White House, 2022), 22, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[11] "Fact Sheet: 2022 National Defense Strategy," Department of Defense, 2, https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF.

[12] Clementine G. Starling, Tyson K. Wetzel, and Christian S. Trotti, *Seizing the Advantage: A Vision for the Next US National Defense Strategy*, Atlantic Council Strategic Paper (Washington, DC: The Atlantic Council, Scowcroft Center for Strategy and Security, 2021), https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Seizing-the-Advantage_A-Vision-for-the-Next-US-National-Defense-Strategy.pdf.

[13] Jim Chen, "On Levels of Deterrence in the Cyber Domain," *Journal of Information Warfare* 17, no.2 (Spring 2018), 32–41.

[14] *National Security Strategy of the United States of America*, 21.

[15] Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation* (Alexandria, VA: Institute for Defense Analyses, May 2018), https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.

[16] Chen, "AI-Based Deterrence in the Cyber Domain," 38–45.

[17] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, (New York: Oxford University Press, 2022), 35.

[18] Ibid., 35.

[19] Ibid., 35.

[20] Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988), 7.

[21] Ibid., 7.

[22] Jim Chen, "Cyber Deterrence by Engagement and Surprise," *PRISM* 7, no. 2, 101–107, https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/9-Cyberdeter-

rence_by_Engagement_and_Surprise.pdf?ver=2017-12-21-110642-140; Jim Q. Chen and Alan Dinerman, "Cyber Capabilities in Modern Warfare," in *Cyber Security: Power and Technology*, ed. Martti Lehto and Pekka Neittaanmäki (Cham, Switzerland: Springer, 2018), 21–30.

[23] Chen, "Cyber Deterrence by Engagement and Surprise."

2

Cross-Domain Cyber Incidents and State Responses

By Michael Navicky and Benjamin Tkach

In July 2021, President Joseph Biden articulated a potential worst-case, cross-domain cyber scenario: the initiation of a shooting war with a major power precipitated by a virtual "breach of great consequence."[1] The probability of a cross-domain spillover event initiated solely by a cyber action is low,[2] but government planning overemphasizes low-probability, high-impact policy planning.[3] Thus, whereas hypothetical zero-day events are frequently referenced, most cyber activity involving cross-domain interactions occurs at lower levels of escalation potential.[4] President Biden's vocalization of the potential cross-domain effects of malicious cyber activity underscores the now nearly decade-long effort by the U.S. Government to develop and institute policies to integrate cyber activity into its policy portfolio.

Despite significant efforts across government, the private sector, and academia, a nebulous cacophony of myriad conceptualizations and operationalizations of cyberspace, cyber attacks, and cyber deterrence has emerged, hindering quantitative research and U.S. policy development.[5] At the same time, cyberspace's relative newness as a cross-domain feature of international engagement has brought into focus the continued relevance and usefulness

of several classic international relations concepts for sharpening our understanding of contemporary cross-domain interactions.

How can cyber contribute to deterrence strategies? Can cyber contribute to cross-domain deterrence (CDD)? Conceptually, CDD is the straightforward integration of cyber activity into the application of national power (for example, DIME—diplomacy, information, military, and economic) applied across land, sea, air, space, and cyber domains to discourage adversaries from specific activities. In actuality, the complexities and challenges of developing and implementing CDD are immense.

The additional complexity of establishing CDD—with multifaceted interactions of virtual and physical world activities affecting outcomes—first necessitates defining deterrence within cyberspace. Yet deterrence in cyberspace remains a contested construct and area of research. Fundamental questions continue to be debated:

- How, exactly, does deterrence in cyberspace differ from deterrence in other domains?[6]
- To what extent can deterrence be manipulated and calibrated?[7]
- Can instances of cyber deterrence be sufficiently well described and verified?
- Is deterrence in cyberspace is even possible?[8]

Fundamentally, deterrence is about signaling to an adversary that certain operations or activities are either too costly to undertake (deterrence by denial) or that undertaking such activities will result in substantial imposed costs (deterrence by punishment). We emphasize the interaction between adversaries because for deterrence to emerge, both the sender and receiver must interpret a signal in a sufficiently similar manner. In the nuclear era, nuclear weapon detonations and delivery vehicle demonstrations effectively established an adversary's capability.

The cyber domain complicates the communication process, because attribution problems obfuscate sender and receiver communications.[9] The lack

of consensus among analysts, let alone adversaries, on how to conceptualize basic features of cyber and its interaction with the physical world has spawned numerous definitions of the cyber domain, cyberspace, cyber campaigns, and cyber attacks.[10] Development of a CDD framework will necessitate clarity of terms and actions; the United States must first understand what it wants to signal before attempting interpretation of adversaries' actions. Nuclear deterrence, even with nuclear weapons' clear destructive capability and ease of attribution, took 13 years after the Soviet Union's first detonation to yield the framework of mutually assured destruction (MAD). Any deterrent signaling involving cyber will be much slower to develop.

Can cyber capabilities signal behavioral expectations between states? Cyber deterrence skeptics rightly argue that cyberspace—with its borderless global operational environment, inapplicability of national sovereignty, varied barriers to entry, and so forth—undermines conceptual features of deterrence.[11] Consistent with the ways deterrence has been studied in other domains, it is useful to acknowledge cyberspace's unique characteristics while differentiating the capabilities used and the domain itself. Cyber is a domain through which multiple types of operations can be conducted (for example, intelligence, surveillance, degradation).[12] Cross-domain signaling is most likely to occur when states use or respond to cyber degradation operations by other states.[13]

We argue that cross-domain responses suggest that states are following the path of prior capability innovations by learning when and how to apply new capabilities. Our analysis differs from prior quantitative efforts, which advanced our understanding of cyber through classification of cyber campaigns, tracking of cyber incidents and military responses, and quantifying cyber's currently limited compellent capacity.[14] Instead, we contextualize cross-domain cyber incidents to analyze the incongruent responses by states.[15] We argue that the limited but increasing number of degradation operations as catalysts of, and responses to, cross-domain state activity suggests cyber's increasing integration into state policy portfolios. These interactions

form the precursors to behavioral norms that need to become established if CDD is to emerge.

We next analyze features of cyber within the context of classic international relations scholarship. This approach enables us to draw on noncyber examples to identify which aspects of cyber are most influential for signaling. First, we show the utility of applying other areas of international politics to cyber when attributing actions to governments, national militaries, and supported paramilitaries. Second, we examine how nuclear deterrence "success" did little to curb competition below the threshold of war. Third, we use historic examples of tactical changes, not simply technological improvements, to demonstrate that advances in cyber defense may track historical patterns and reduce, though not eliminate, current offensive advantages. Fourth, building on the theoretical literature, we show that state interactions in cyberspace can convey meaningful signals even in the absence of attribution certainty. We then analyze cyber incidents that precipitated disproportionate state responses to extrapolate how signaling is an ongoing process across domains. We conclude with implications from our research and avenues for future efforts.

Cyberspace, Cyber Operations, and International Relations

The evolution of cyber concepts is being outpaced by the integration of the physical and virtual worlds. Initial debates, as is consistent with other disciplines, concentrated on defining terms as scholars and practitioners developed idiosyncratic nomenclatures to describe specific aspects of cyber activities.[16] While many debates continue, we use the Department of Defense (DOD) conceptualization of cyberspace as consisting of three layers:

- connections in the physical world (hardware)
- digital connectivity (networks, protocols, procedures)
- actor profiles (humans or automated entities).[17]

We draw on classic international relations concepts and theories to examine how assumptions in cyber literature can complicate or impede analysis of cyber's efficacy in international interactions. First, we argue that differentiating between types of cyber activity based on their technical sophistication and resource intensity elevates the role of the state and its capacity to organize and leverage personnel, resources, and connectivity. While there is a low barrier to entry for most cyber activities,[18] degradation attacks that destroy, sabotage, or disconnect systems, networks, or operations are more resource intensive.[19]

Second, we argue that the current cyber defense deficit—relative to offensive capabilities—will narrow over time as cybersecurity practices improve at the individual and government levels. Defense capabilities will improve as defensive tools emanate from the private sector, standardized cybersecurity requirements (that is, the DOD Cybersecurity Maturity Model Certification, zero-trust structure) are implemented, and individual cyber hygiene solidifies.[20] Third, we argue that attribution difficulties are not an insurmountable impediment for cyber policy. Instead, levels of certainty across the attribution spectrum enable policy decisionmaking in the presence of uncertainty. Fourth, we argue that critics of cyber deterrence rightly identify that nuclear weapons and cyber activity are distinct and that direct parallels have limited comparative utility.

However, we argue that the extensive violent and nonviolent competition below the threshold of nuclear war during the Cold War foreshadow a similar dynamic emerging in the cyber domain, with actors intentionally avoiding the worst-case scenario of an accidental debilitating cyber incident, thereby providing opportunities for cyber to contribute to CDD. Development of capabilities to conduct and defend against degradation attacks requires state resources and constitutes a high priority for U.S. policy leaders. We draw on classic conceptualizations of uncertainty to argue that a continuum of confidence in attribution is sufficient to allow for signaling interactions to emerge.

States, Cyberspace, and Resource Management

One argument against cyber's potential contribution to deterrence is that the low barrier to entry enables a plethora of actors to conduct cyber activities. Cyberspace structure—with its lack of regulations, prominence of anonymity, and diffuse connectivity, for instance—is such that the proliferation of actors engaging in cyber activities is theoretically infinite. Conceptually, cyber participants are divided into three categories: states, nonstate actors affiliated with states, and nonaffiliated nonstate actors. Dividing cyber actors in this manner enables us to examine how states, through their militaries, intelligence agencies, and sponsored paramilitaries, marshal resources necessary to conduct attacks that are most likely to escalate across domains.[21] Not all cyber activities require the same mobilization of resources. Consequently, we make no assumptions that nonstate actors do not possess cyber capabilities or the capacity to steal and utilize capabilities. (For example, the 2017 WannaCry ransomware attack is purported to have originated from the National Security Agency.) Rather, by emphasizing the state, we prioritize near-peer global competition where adversaries' repeated interactions may enable signaling to emerge.

Emphasizing the state in cyberspace places cyber activity in the broader context of state interactions. Historically, war is a centralizing activity of state formation, so cyber was first broadly analyzed within the context of war in the physical domain.[22] Some scholars argue that hostile cyber activity is likely to provoke kinetic responses only when it happens in the context of an ongoing shooting conflict.[23] Several cyber scholars anticipate limited effects of cyber activities in conflict, relegating the potential impact to sabotage operations,[24] deception,[25] or information campaigns. Early empirical research seems to confirm the view that cyber has limited effects on the battlefield.[26] Others note that compellence in any domain is difficult, and cyber compellence is particularly so because of attribution difficulties and a lack of cross-domain effects.[27]

But cyber activity is also a form of signaling—communication—between adversaries. Consolidating state-sponsored actors into a unitary-actor frame-

work is consistent with state application of political power to achieve policy objectives. International relations scholarship effectively connects proxies with their state sponsors. Paramilitary activities, civilian victimization,[28] and state-sponsored terrorism[29] are studied within this unitary-actor framework. According to William Akoto, in cyber-specific contexts, a state's decision to delegate cyber operations to nonstate cyber proxies is conditioned by domestic political accountability considerations.[30] Specifically, despite the ease with which cyber activities can be outsourced to proxies, the potential liability exposure of the government if cyber operations go wrong is a determining factor in the use of proxies.[31] In effect, domestic political accountability can act as a constraint on the use of cyber proxies. In autocratic regimes, such as Russia and China, where accountability mechanisms connecting the people and the government are limited (or absent), cyber proxies are more likely to be used by the state, under the pretext of deniability. However, by Akoto's logic, states with limited political accountability are those with the least plausible deniability for the activities of their proxies—which effectively connects the proxies with their state sponsors. For example, the United States implemented sanctions against the Russian state for activities associated with the SolarWinds cyber breaches by Russian nonstate operatives.[32]

State marshalling of resources and personnel is essential for many types of cyber activity the United States seeks to deter. From a policy perspective, the current National Security Strategy emphasizes the capabilities of peer and near-peer adversaries. Similarly, the 2015 Department of Defense Cyber Strategy specifically sought to develop a strategy to deter state actors from targeting U.S. interests in cyberspace. Conceptualizing the state and its affiliates as a single actor facilitates comparisons of attacks consistent with U.S. national strategy approaches. For example, Brandon Valeriano, Benjamin Jensen, and Ryan Maness argue that because the United States is the world's latent cyber capacity leader (Valeriano, Jensen, Maness 2021), it conducts degradation operations at a higher-than-expected rate.[33] States and state-supported actors benefit from the resources and bureaucratic infrastructure that facilitate cyber capabilities.[34]

Cyber Defense Improvements and Historic Tactical Evolutions

Cyber critics frequently argue that current cyber defensive capabilities are too porous for deterrence by denial to be effective. But it is much too early in the evolution of cyberspace to declare defensive capabilities eternally ineffective. As a dynamic environment, cyberspace seems unlikely to develop in a straight line. Rebecca Slayton argues that identifying the balance of offense and defense is more complicated in cyberspace than in other domains, requiring dynamic, dyadic-based comparative analysis.[35] She argues that offensive cyber is currently comparatively cost intensive compared with defense and shows that sunk costs of the Stuxnet offensive attack were less of a concern than operational objectives. Ben Garfinkel and Allan Dafoe start with the expectation that offensive capabilities will dominate defensive ones; they then develop a theory of offensive-then-defensive scaling that integrates emerging technologies such as artificial intelligence to demonstrate how offensive capabilities can be leveraged to achieve improved cyber defense.[36] They predict that current offensive advantages will migrate to defenders: deception by actors in cyberspace applies to both attackers and defenders. Defenders can utilize concealment to entrap an attacker, whereas attackers' covert activity against sophisticated opponents must avoid attribution.[37] The extensive literature on the cyber offense-defense balance predominantly focuses on technical features of cyberspace to decipher its future development. Technology will undoubtedly change cyber defense capabilities. Yet historic noncyber and nonnuclear examples of tactical innovations shifting the offense-defense balance demonstrate how tactical changes affect military operations.

Prior noncyber tactical adjustments and innovations suggest that current assumptions about cyber may not hold over time. We draw on two aviation examples to demonstrate this perspective. First, drawing from the early era of airpower, we consider Stanley Baldwin's 1932 argument that "the bomber will always get through."[38] Baldwin's theory was based on the adoption of tactics that leveraged the U.S. B-10 bomber's speed advantage over adversaries' intercept aircraft. Tactical considerations, and not just technological capabilities, guided the debate between American and British generals about

the relative benefits of risky daytime precision versus safer nighttime bombing. Nighttime bombing proved to be less accurate; daytime bombing risked significant losses. In fact, the Eighth Air Force lost so many bombers in August and October of 1943 that it suspended long-range bombing. The substantial losses offered evidence that, in fact, the bomber would not always get through.

Second, early theorists of the employment of the airplane proposed not engaging an enemy's armed forces. Gérard Chaliand proposed limiting targeting to "the centres of all [the enemy's] systems of communications and transportation, his docks and shipyards, railway workshops, wireless stations, and postal and telegraph systems."[39] On the other hand, bombers in mass provided the ability to destroy the "interior of an enemy's country so devastatingly that the physical and moral resistance of the people would also collapse."[40] Tactical thinking about daylight bombing runs evolved but brought with it massive losses in human lives and aircraft.

The Army Air Force, the lone champion of daylight precision bombing during World War II, moved away from daytime bombing after the war. The modernization of the Law of Armed Conflict—prohibiting Douhet's approach[41]—combined with the invention of guided missiles and radar technology meant that the bomber had a harder course to navigate. Given the technology and tactics of Baldwin's 1930s era, bombers indeed got through. Today, recognition that bombers may not get through suggests that broad assumptions early in a period of transformation may not hold over time. The assumption that cyber defenses will always remain porous may look antiquated in a decade or two.

Although no defense is perfect, Federal defensive cyber capabilities are likely to improve over time. Since the 2009 Comprehensive National Cybersecurity Initiative, the executive branch and later Congress have actively pursued defensive improvements. DOD's Cybersecurity Maturity Model Certification (CMMC) includes a means to protect the defense industrial base through adherence to cybersecurity standards. CMMC 2.0 requires defense contractors to achieve one of three levels of certification prior to bidding

on requests for proposals. Implementation of cybersecurity standards and continuing collaboration with DOD includes cybersecurity capabilities, a big improvement over prior efforts to simply stick on cyber considerations. DOD is also implementing zero-trust procedures to protect its own networks.[42] Although the Government Accountability Office has identified that prior cybersecurity efforts in DOD require additional improvements, broad recognition of cybersecurity's importance and quantification of results show how far integration of defensive postures has progressed.[43] Over time, changes to the foundational cyber infrastructure will improve resiliency—even as they leave unchanged the need for active defensive policies, the possibility of a breach, and the importance of continually educating people about cybersecurity.[44]

Improvements in the U.S. capacity to deter adversaries through denial elevates the importance of cross-domain interactions. Deterrence is fundamentally about signaling a credible response capability and communicating with an adversary. Somewhat counterintuitively, increasing the cost of conducting offensive cyber and cross-domain operations involving cyber improves the quality of the communication between adversaries. As defensive capabilities improve, only adversaries willing to expend significant resources are likely to conduct cyber-involved cross-domain operations. The narrower range of potential adversaries improves the likelihood of accurate attribution.

A brief history of bank robberies in the United States shows how defensive improvements shortened the roster of potential adversaries and thus improved attribution. Many historians identify the bank robberies conducted by Jesse and Frank James and their accomplices in 1866 as the first in a wave of robberies that swept west after the Civil War. Since then, the evolution of security technology and tactical changes adopted by police have greatly reduced the frequency of bank robberies and increased successful prosecutions.

Defensive cyber may evolve in the same way, with incremental improvements in deterrence gradually reducing the frequency of attacks, though without ever eliminating them. The reduced frequency of attacks may enable defenders to concentrate on attribution and retaliatory responses. Just as happened with bank robberies, defense improvements—deterrence by denial

and the ability to attribute attacks—will communicate to future potential perpetrators that hostile activities will have a high cost.

State Interaction and Attribution in Cyberspace

The proliferation of cyber entities—states, individuals, organizations, bots—and the structure of cyberspace underpin the difficulty of attributing actions to specific entities. Attribution of an action to a specific actor—or set of actors—is fundamental to signaling models and, ultimately, deterrence. Deterrence necessitates that actors establish credibility with adversaries that an attack will generate a response. It also requires actors to identify which actions they seek to deter—that is, which actions they will count as constituting an attack.

Initially scholars argued that the attribution problem, as it became known, is fundamental to cyberspace and reduces the effectiveness of deterrence by punishment.[45] In this framework, deterrence by punishment, perhaps most emphatically articulated in MAD, cannot be implemented in cyberspace, because the difficulty of identifying the source of an attack may delay a response or ultimately negate taking action.[46] If the attribution problem is sufficiently severe that deterrence by denial is the only option, then cyber competition is essentially a resource availability and management competition. Under this scenario, cyber defensive capabilities are the only plausible policy for states, regardless of the adversary and action to deter. Yet the assumption that attribution cannot be improved in turn assumes that future technical changes will always favor the attacker and that perfect attribution is necessary for deterrence to emerge.[47] Both are problematic assumptions.

The following section traces how attribution limitations in noncyber domains demonstrate that cross-domain conditions enable some features of deterrence to emerge in the absence of perfect attribution—namely, retaliatory credibility and the identification of behaviors to deter. To develop these points, we first examine the difficulty of establishing attribution even in conventional warfare. Covert and clandestine operations intentionally are undertaken to obfuscate responsibility and avoid potential escalation. Second, we examine

the theoretical literature's insights into cyber deterrence in the absence of total attribution. In brief, game modeling demonstrates that deterrence signals can be sent and received even in the absence of attacker attribution or signal clarity from the defender.

Attribution in conventional settings is not straightforward, because states intentionally obfuscate their activities. Covert operations intentionally conceal a perpetrator's identity; clandestine operations conceal the activity itself. Arguably, states conduct covert or clandestine operations when escalation is likely to occur if an adversary discovers the perpetrator or operation. As is the case with cyber operations, attribution of conventional covert and clandestine operations is difficult and time consuming. Yet even when major powers identify that an adversary is conducting activities, they may deliberately keep the activity secret. Austin Carson theorizes that this "tacit collusion" between adversaries generates a "backstage" where states may compete, and aggressively so, while limiting the risk of escalation.[48] The process of assigning attribution in covert and clandestine operations shares characteristics with the attribution process required by cyber actions, and these shared characteristics enable useful comparisons. Given their sophistication and resource requirements, covert and clandestine operations by their very nature frequently limit the number of potential perpetrators. Similarly, the resources and organizational infrastructure required to mount many cyber operations limit the number of possible suspects for any given incident.

Second, state interaction in cyberspace offers opportunities to communicate with adversaries, even when attribution is not certain. Attribution is just one of many forms of uncertainty that affect decisionmaking processes and international interactions. Attribution in the cyber domain is currently significantly more difficult to establish than in the nuclear weapons case, but that is a poor rationale to assume that attribution in cyber cannot be improved or that states will not learn to incorporate uncertainty about attribution into their policymaking. Social science methods are particularly well suited to research questions centered on how uncertainty affects decisionmaking and

interaction among actors. Emerging research demonstrates the feasibility of deterrence in situations where attribution is not absolute.

In these theoretical models, typically two belligerents engage in a sequence of interactions that generate multiple potential equilibriums—the solution set(s) where both players select the best strategy given the decisions of the other player. One article, by Sandeep Baliga et al. shows that deterrence can occur without perfect attribution.[49] In their model, the authors suggest that there are several possible attackers and the defender seeks to retaliate against only the actual attacker. In brief: a defender's retaliatory capability is public knowledge, and potential attackers adjust policies on the basis of signals from the defender. The authors further find that the defender can effectively increase deterrence by committing to a strategy before an attack occurs and publicizing the chosen strategy. Thus, the defender's credibility about launching a retaliatory attack overcomes limitations in attribution by signaling the costs of a potential attack. Retaliatory credibility does not remove attribution hurdles, and defenders must adopt policies to strengthen deterrent effects. The authors recommend efforts to reduce false alarms and improve attack detection as initial steps defenders can take to bolster deterrence. They moreover caution that defenders that are unable to identify attackers over time or that require a high level of attribution certainty before retaliating risk weakening deterrence effects.

Defenders who absorb cyber attacks can generate deterrence against future attacks both through signaling and, paradoxically, by receiving more attacks (which improves attacker identification).[50] In the model developed by Jonathan Welburn, Justin Grana, and Karen Schwindt, cyber retaliatory capability is private information—it is known only to the defender. There is only one attacker in this model, though the defender still cannot perfectly attribute attacks. Critically for deterrence, this model enables analysis of how defenders signal attackers and answers the question "Does signaling in the cyber context convey meaningful information from defender to attacker?" Welburn, Grana, and Schwindt demonstrate that a babbling equilibrium emerges, but defenders can still convey information in the equilibrium. Con-

ceptually, noisy signals occur when a sender's message is garbled or misinterpreted by the receiver. The significant insight here is that noisy signals about retaliatory capabilities, either publicly announced or privately demonstrated, eventually generate deterrence. Thus, deterrent signaling occurs in the absence of perfect attribution.

In sum, attribution remains a serious but addressable issue for CDD. Improvements in retaliatory capability increase the possibility of deterrence. States and entities can also increase their understanding of adversaries and mastery of their own strategies to improve deterrent effects.[51] By demystifying the ways attribution affects signaling and deterrence, the theoretical literature demonstrates that the hurdles to cyber deterrence are only partly technical in nature (for example, tracking, tracing, identifying). And, although solving the technical issues of attribution is critical, the uncertainty emerging from attribution problems is amplified in the interactive context of international politics. States and other actors manage uncertainty across many issue areas and activities, and it is reasonable to expect that cyber interactions will join the cross-domain interactions of the international system. Perfect attribution is likely not attainable, and we expect actors to adjust policies to reflect the uncertainty.

Cyber Signaling and Global Competition

We next highlight two features from the early era of nuclear deterrence that apply to the cyber domain. First, deterrent success during the Cold War was restricted to worst-case scenarios; nuclear weapons did not prohibit—and may indeed may have incentivized—competition below the threshold of war. Second, nuclear-armed states and their adversaries learned how exactly the threat of nuclear war conditioned militarized engagements (or did not). Applying these two observations to cyber, we argue that cyber deterrence success is more akin to avoiding the worst-case scenario than to achieving the complete cessation of aggressive cyber activities. Consequently, cyber campaigns may in fact reflect recognition by states that behavioral norms are developing below the threshold of conflict. Second, we argue that, as is con-

sistent with other martial innovations, states are increasingly learning how to employ cyber to pursue policy objectives and increasingly willing to use degradation incidents to signal policy priorities. Degradation incidents are pertinent for signaling because they are more escalatory, potentially heightening signaling utility among competing states.

Applicable parallels between nuclear and cyber deterrence are limited, but the fact that competition has flourished in the presence of nuclear weapons is relevant to cyber. Like nuclear deterrence, deterring cyber incidents may involve avoiding only the worst-case scenarios. Competition below the threshold of conflict will flourish, as it did during the Cold War. Dyadic competition then included nonviolent areas such as sports (for example, alternating Olympic boycotts), space, and chess. Militarized competition involved patrons and proxies across dozens of engagements on multiple continents.[52] The entire period, in fact, is defined by competition, including conflicts such as the Korean War, which in 1951 involved dogfights directly pitting U.S. against Soviet pilots.[53] Mark Bell and Nicholas Miller ague that dyads with both members possessing nuclear weapons are not significantly less likely to fight wars and that dyads where only one state has a nuclear weapon are more prone to low-level conflicts short of war.[54] Deterrence during the Cold War had a zero-tolerance policy for only one action—nuclear weapon use. Cyber deterrence may evolve along similar lines, avoiding accidental escalation while enabling robust communication and competition.

Extensive competition dynamics facilitate signaling between adversaries across domains. Building on an argument that deterrence is most likely to succeed only when signaling between adversaries establishes behavioral expectations,[55] we argue that degradation attacks that elicit a cross-domain response are most interesting because of the complexity necessary to establish resolve and credibility in a cross-domain context.[56] In this context, the extensive interactions below the level of conflict are necessary interactions for states to establish signaling norms and meanings. Consequently, cyber's role in deterrence is likely to emerge only as states develop expectations and norms across the full continuum of cyber actions. But because cyber has a

limited compellent effect[57] and problems of attribution are significant, interactions involving degradation are the most interesting for signaling purposes. Degradation attacks and state responses to such attacks frequently involve a destructive component that crosses the virtual/physical threshold. Such attacks are therefore more likely to convey information about resolve and capability between participants than other types of cyber engagements.

Degradation attacks involve destruction or sabotage of enemy networks, operations, or systems.[58] Degradation attacks are costly, require specific targeting, and may or may not knock out a target for a sustained period. However, because degradation attacks involve significantly more sunk costs and are thus more likely to be enacted by states, they may signal to adversaries more effectively than other cyber activities. Degradation attacks did not start until well after other initial cyber espionage and intelligence incidents, according to a particular dyadic dataset.[59] Indeed, the frequency of degradation attacks remained low throughout the 2000–2014 period, ranging from one to five incidents per year after 2005.

We see a similar pattern of low but continual use in the Center for Strategic and International Studies (CSIS) database of significant cyber incidents from January 2006 through September 2022. We coded the 903 identified cyber attacks from this period into the following categories: criminal, espionage, information, jamming, and destructive. Destructive cyber events are those where the cyber incident itself or the response to the incident crossed domains, resulting in the degradation of physical or cyber capabilities.[60] Destructive cyber incidents accounted for only approximately 7 percent of all incidents, though there was a small increase in frequency after 2016. The 63 destructive incidents counted suggest that both the United States and its adversaries are slowly increasing their use of destructive cyber capabilities or increasingly responding to cyber incidents with destructive responses in the physical world.

While clearly not yet establishing deterrence, the choice by states to employ destructive cyber attacks or respond to such attacks with physical use of force suggests that states are learning how, when, and against whom to use

destructive cyber capabilities. Given the complexities of cyber and the intricacies of cross-domain activities, a steep learning curve by states about when and how to employ cyber should be expected.

In sum, states continue to adjust policies and their responses to cyber capabilities below the threshold of armed conflict. If cyber is to contribute to deterrence, we should expect continued extensive engagement as states learn how to use and respond to cyber incidents, particularly degradation attacks. Although parallels between nuclear and cyber deterrence are imperfect and problematic, the literature on nuclear weapons nevertheless gives us insights into how states handle, and adversaries respond to, new capabilities.

Vipin Narang shows that states pursuing nuclear weapons are more likely to experience conflict up to the point of proliferation, and then conflict likelihood drops.[61] Michael Horowitz shows that whereas the process of acquiring nuclear weapons increases the likelihood of conflict initiation and reciprocation of conflict, over time the possession of nuclear weapons decreases the likelihood of conflict.[62] Adding helpful nuance to this picture, Kyung Suk Lee et al. found that possessing nuclear weapons decreases the likelihood of low-level military conflict with a non-nuclear-armed adversary, but between nuclear-armed dyads there is no effect on the likelihood of military conflict.[63] Moreover, Narang demonstrates that it is not the possession of nuclear weapons per se that affects conflict dynamics.[64] Rather, it is different nuclear postures that shape engagements. When applied in a cyber context, these studies suggest that states gradually learn when, how, and against whom to utilize new capabilities. We expect nothing different in the case of cyber capabilities. Cyber's short history may or may not reflect how cyber capabilities are likely to evolve over time, and we argue that changing responses to cyber and cyber-enabled actions are indications of developments in state signaling dynamics that are already under way.

Cyber and Cross-Domain Incidents

We now examine four notable cross-domain cyber-involved incidents to evaluate how cyber contributes to signaling. Consistent with CDD, cyber

attacks can initiate a crisis or be implemented in response to an action in one or more of the other domains (land, sea, air, and space). Establishing deterrence in any context requires establishing a credible response and effectively communicating with adversaries to identify the specific behaviors the sender seeks to deter. States in the international system are in the early stages of establishing cyber norms and expectations. Consequently, how the United States and other states initiate and respond to cyber incidents communicates expectations to adversaries—and vice versa. By aggregating individual incidents, states can begin the process of developing and then refining deterrent messaging through repeated interactions. Aggregated cross-domain incidents accumulate meaning, and though in this section we review just three example incidents, the described process may contribute to CDD as states' interactions evolve.

The examples we chose articulate how the four insights presented in the preceding sections—the utility of state-centric analysis, the likelihood of improvements in defensive cyber, the possibility of policymaking in the face of attribution uncertainty, and the potential of cyber signaling—are reflected in recent cross-domain interactions. Clearly, these examples do not demonstrate CDD; rather, they capture how a government may respond to an adversary's behavior in a cross-domain context. We do not attempt to draw specific lessons of deterrent norm creation from individual incidents, unless a state clearly articulates that a response is designed to deter future behaviors, as was the case for the 2018 U.S. cyber operation against Russia operators associated with attacks on the 2016 Presidential election. Instead, the analyzed interactions may best be seen as precursor events, necessary for signaling to occur.

First, in May 2019 the Israeli Defense Forces and Hamas engaged in cross-domain warfare involving a cyber attack. We begin with this example because the two governments are engaged in a long-standing rivalry, and Hamas's cyber activity generated a kinetic response from Israel. Hamas attempted to hack unspecified targets in Israel—a continuation of the ongoing animosity between the actors. Israel responded by launching an air strike. Israel's response in the air domain, announced via Twitter, clearly means that

attribution of the cyber attack to Hamas exceeded attribution uncertainties frequently cited as hindrances to cyber signaling and deterrence.

The use of a kinetic response to a cyber attack is a rare event—not only for this rivalry but also for cyber incidents in general.[65] We count more than 900 significant cyber incidents on the CSIS list, and only 2 received a kinetic retaliation, one a precision strike targeting an individual, the other a major airstrike on a building complex. In fact, the rarity of kinetic responses to cyber actions strengthens our contention that actors are currently experimenting with signal efficacy across different domains. Hamas has conducted numerous cyber operations against Israel, yet this one is the only event that generated a kinetic reprisal. In addition to any degradation objectives associated with the air strike, Israel apparently wanted to signal that the type of cyber operation Hamas undertook was unacceptable and would be met with force. In short, Israel's airstrike response signaled retaliatory credibility and demonstrated attribution confidence. In a signaling context, these interaction features are the necessary initial steps to establish CDD.

Second, in October 2018 U.S. Cyber Command (USCYBERCOM) began targeting individual Russian operatives who were attempting to interfere with U.S. elections and spread disinformation. The details of USCYBERCOM activities and methods were not disclosed, but former officials indicated that the Russian operatives would understand they were being targeted. This is an example of an information operation conducted through cyberspace—which is an important distinction. The most important aspect of this example is that the operations were conducted to deter election interference and the spread of disinformation. Consistent with our fourth implication—that signaling can occur without perfect attribution—these interactions illustrate how actors can take additional steps to enhance signal efficacy. In this case, the U.S. public's awareness of actions, along with removing attribution ambiguity for the Russians, elevated the clarity of the message. The deliberate public disclosures suggest that the operation was designed in whole or in part to signal U.S. preferences, given that the nature and outcome of USCYBERCOM activities are classified.

Third, in June 2019 Iran claimed that a drone, a U.S. Navy RQ-4, violated Iranian airspace. Iran responded by downing the drone with a surface-to-air missile. Reports suggest that an initial retaliatory kinetic strike was planned, but the United States ultimately decided to respond with a degradation cyber attack that disabled the control systems of Iranian rocket and missile launchers.[66] The cross-domain application in this example exemplifies the state-centric feature of CDD. In the context of the enduring rivalry between the United States and Iran, the ability of the United States to have offensive cyber options available as a policy alternative is unlikely to be duplicated by nonstate actors. The ease and timeliness of the U.S. response suggests that the utilized cyber capability was previously developed and was being held in reserve. The decision to reduce the response from kinetic to cyber suggests that the U.S. perceives cyber degradation attacks as carrying information in signaling but not the escalatory liability of kinetic strikes. The example also demonstrates that the United States is actively communicating preferences and conducting retaliatory operations to signal adversaries about U.S. preferences.

Furthermore, this example supports our contention that cyber signaling is an ongoing process. The U.S. public announcement claiming responsibility for the degradation incidents illuminates two features of cross-domain interactions. First, while communication without perfect attribution is possible, the United States chose to establish clear deterrent implications from its activity. Consequently, it publicly announced the cyber activity to ensure that Iran received the message. Interestingly, the United States did not state that the way the degradation activity was executed would itself reveal U.S. fingerprints, as the U.S. had announced in its 2018 operations against Russian operatives. Second, the United States likely sought to deescalate tension in its contentious rivalry with Iran by opting for a cyber response instead of a kinetic one. This decision clearly demonstrates that states consider the multidimensionality of cross-domain activities when selecting retaliatory responses. It would of course be misguided to draw any broad lessons from a single interaction about the value the United States sets on its drones and how it calibrates the severity of cyber degradation attacks. Instead, for our

purposes, this example clearly shows state actors integrating cyber into their policy designs and, currently at least, viewing cyber actions as less of an escalatory risk than other options.

Finally, it is worth reviewing a well-known cyber incident through the lens of CDD: the North Korean hack of Sony. This incident is worth discussing because it clearly represents two nation-states in conflict within the cyberspace domain. Although North Korea has never accepted responsibility for the attack, the Federal Bureau of Investigation has definitively attributed it to North Korea. Additionally, in 2018 the Department of Justice filed formal charges against a North Korean operative, Park Jin Hyok, in the attack. The attack was conducted in November 2014 by a group called "Guardians of Peace" and sponsored by the North Korean government. The group defaced employee computers and, more important, exfiltrated massive amounts of confidential and proprietary data. The stolen data included employee personnel records and salaries as well as data on future films and private emails. It is clear the loss of these data had significant negative externalities for Sony, affecting both its public image and financial standing. The attack's motivation apparently traced back to the North Korean leader Kim Jong-un, who aimed to prevent the release of *The Interview*, a comedy featuring an assassination attempt against the North Korean leader. Given this goal, the North Korean cyber attack was largely successful. Several theater chains decided not to show the movie, and Sony significantly modified the release schedule of the film.

North Korea's attack and the U.S. response constituted an interactive cross-domain signaling effort. The incident provided notice to moviemakers everywhere that there are limits to what North Korea will tolerate, although those limits may not be completely clear. In response to this attack by North Korea, Washington implemented economic sanctions, and President Barack Obama further stated, "We'll respond proportionally, and we'll respond in a place and time and manner that we choose."[67] The actions and words from the United States were clearly intended to deter future attacks on U.S. targets. North Korea's cyber coercion was limited, but the concrete response by Sony and the United States to a cyber-initiated incident demonstrates

the ongoing cross-domain interactions and policy calculations by state and nonstate actors.[68]

The analysis provided in this section is just a first step toward evaluating how cross-domain incidents establish retaliatory credibility and signal which behaviors states seek to deter. Significant additional research is necessary on the dynamic, dyadic interactions of states across domains. The complex adaptiveness and ease of proliferation—of both actors and abilities—heightens the risks associated with operations in cyber as actors operate for the time being with fewer constraints than in other domains.[69] Our cursory foray indicates the feasibility of cross-domain signaling involving cyber. The full emergence and articulation of CDD remains years away, as states gradually codify what is and is not acceptable through repeated interactions.

Implications and Conclusions

Cross-domain events that start in cyberspace or are responded to with cyber capabilities fundamentally comprise the necessary components of deterrence. We establish that cross-domain incidents satisfy the communication requirement for deterrence to emerge.[70] Our research highlights cross-domain events to contextualize how signaling capabilities between adversaries may evolve. The extensive amount of competition below the level of conflict, not only in the military sphere but also across attributes of power (DIME), requires adoption of different metrics with which to evaluate how cyber activities affect signaling. As states continue to employ cyber capabilities, clarity of signaling and deterrent messaging will improve.

The United States is positioning itself to fully integrate cyber offensive operations into its cross-domain capabilities. National Security Presidential Memorandum 13 (NSPM-13), *United States Cyber Operations Policy*, signed during the Donald Trump administration, pushed decisionmaking authority to use offensive cyber capabilities below the President. In essence, the memorandum granted military commanders more autonomy about when and how to use offensive cyber capabilities. While clearly falling short of President Harry Truman's infamous, poorly chosen words, "The military commander

in the field will have charge of the use of the [nuclear] weapon, as he always has,"[71] the classified NSPM-13 reportedly provides the military additional flexibility to conduct offensive cyber operations without interagency approval from the Department of State. The Biden administration has signaled it intends to modify the order, potentially reinstituting an interagency requirement.[72] Still, even if additional freedom-of-action restrictions are implemented, NSPM-13 is a clear sign the United States intends to integrate offensive cyber capabilities into its arsenal of world-leading cross-domain capabilities. On the basis of our analysis, we expect offensive cyber operations to hasten CDD as adversaries are engaged in a timely, flexible, and effective manner in response to their activities.

Future analysis should concentrate on degradation operations and state responses. Deterring degradation attacks should be a U.S. priority, and this area is worth examining for several additional reasons. First, cyber operations involving disruption and espionage by other states are more applicable to deterrence by denial insofar as they define a threshold below degradation operations. Second, within a deterrence signaling framework, degradation actions in cyberspace may elicit a response from the target, thus generating engagement between the actors. In brief, degradation attacks are the most likely cyber activity to immediately escalate across domains as national security capabilities are impaired, constricted, or destroyed. Further analysis of degradation attacks and state responses is necessary to fully unpack the generation of CDD.

Scholars have yet to apply the intelligence community's approach to uncertainty to the cyber domain. The intelligence community's process to produce levels of confidence in the presence of uncertainty is a useful guidepost for cross-domain activities involving cyber. Standardizing the process by which actors classify uncertainty, particularly regarding attribution, will generate a consistent framework for policymaking. The determination of confidence levels may emerge as a necessary condition for CDD's development to facilitate retaliatory decisionmaking. Policymakers and analysts may have to accept that generating deterrence requires weighing the costs and benefits of

retaliatory responses while uncertainty regarding the identity of the perpetrator remains. Additional research developing and applying levels of confidence frameworks to different cross-domain scenarios is necessary in a world where perfect attribution is unlikely.

Cyber's role in CDD is essential if we are to avoid Robert Jervis's least stable "world": a world where offense has the advantage and an offensive posture is indistinguishable from a defensive one.[73] As we have suggested, an isolated cyber incident triggering a major conflict is a low-likelihood event, but given President Biden's voicing of that exact concern, CDD offers opportunities to exit the least stable world. Through improvement of deterrence by denial, offensive advantages in cyber can be reduced. More critically, by establishing cross-domain deterrent expectations with adversaries, states will become better able to distinguish between offensive and defensive postures. Conceptually, adversaries generate red lines that demarcate where competition can still occur, while establishing that crossing the red lines would signify a different posture. Additional research extending our examination of disproportionate state responses will aid in identification of cyber postures. Jervis argues that the world where offense is advantaged but postures can be differentiated lacks the security dilemma but allows aggression to remain possible. And because aggression remains possible and CDD, even under the best of scenarios, will not be a zero-tolerance policy in cyber activity, the United States must continue to strive to sustain its cyber advantages.

Notes

[1] Joseph Biden, "Remarks by President Biden at the Office of the Director of National Intelligence," July 27, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/.

[2] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013), 41–73, https://www.belfercenter.org/publication/myth-cyberwar-bringing-war-cyberspace-back-down-earth.

[3] John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (New York: Free Press, 2006).

[4] Brandon Valeriano and Benjamin Jensen, *The Myth of Cyber Offense: The Case for Restraint*, Policy Analysis No. 862 (Washington, DC: Cato Institute, 2019), https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint.

[5] Jacquelyn G. Schneider, "Deterrence in and Through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon R. Lindsay and Erik Gartzke (New York: Oxford University Press, 2019), 95–120.

[6] Nadiya Kostyuk, "Deterrence in Cyber Realm: Public Versus Private Cyber Capacity," *International Studies Quarterly* 65, no. 4 (2021), 1151–1162; Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

[7] Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* 44 (August 2021).

[8] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), 381–393; Richard J. Harknett, John P. Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010), 1–24.

[9] Lorraine Finlay and Christian Payne, "The Attribution Problem and Cyber Armed Attacks," *American Journal of International Law Unbound* 113 (2019), 202–206; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015), 4–37; Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (2012), 229–244.

[10] Schneider, "Deterrence in and Through Cyberspace"; Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," *Journal of Peace Research* 51, no. 3 (May 2014), 347–360.

[11] Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace."

[12] For comparison, using the air domain as an example, we note that air is a domain through which a range of military operations are conducted. Examples of such operations include airspace denial operations, precision ground strikes, airlift missions, and surveillance and reconnaissance missions.

[13] In areas such as cyber espionage and information campaigns, deterrence is less likely to emerge at lower thresholds of engagement, for a couple of reasons. First, the attack surface area, particularly for information campaigns, is enormous, with multiple entities that are unlikely to synchronize efforts. For example, Jelena Vićić argues that part of Russia's meddling in the 2016 U.S. general election involved spreading truthful statements. Second, deterrence, as commonly used in reference to nuclear weapons, is a strategy that seeks to avoid the worst-case scenario while allowing significant, sustained competition at lower escalation points. See Jelena Vićić, "The Other Means? Examining

the Patterns and Dynamics of State Competition in Cyberspace" (Ph.D. diss., University of Cincinnati, 2021).

[14] Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies* 45 no. 4 (2020), 534–567, https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354.

[15] Valeriano, Jensen, and Maness, *Cyber Strategy*.

[16] See Schneider, "Deterrence in and through Cyberspace," for a summary of conceptualizations within cyber literature.

[17] We draw specifically from Joint Publication (JP) 3-12 to define *cyberspace*. JP 3-12 establishes that cyberspace consists of three interconnected layers, including physical networks (hardware), logical networks (connectivity of the physical networks), and personae (networks of human or automated accounts abstracted from the logical networks, that is, profiles). See JP 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, 2018), xv-I-5.

[18] Valeriano, Jensen, and Maness, *Cyber Strategy.*

[19] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber Warfare," *Survival* 53, no. 1 (2011), 23–40; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013), 365–404. Nonstate actors have conducted degradation attacks. Notably, global, pervasive attacks by nonstate actors may draw on capabilities initially developed by states. This likely occurred in the Petya attacks, which drew on EternalBlue exploits allegedly developed by the National Security Agency. Additionally, the NotPetya attacks specifically targeting Ukraine were orchestrated by Sandworm, a hacking group affiliated with the Russian GRU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation).

[20] Charles W. Mahoney, "Corporate Hackers: Outsourcing U.S. Cyber Capabilities," *Strategic Studies Quarterly* 15, no. 1 (Spring 2021), 61–89, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-1/Mahoney.pdf.

[21] We do not intend to downplay the threat posed by nonstate actor cyber activity to the U.S. Government or the private sector. Instead, we suggest that not all cyber threats and activities are the same. Some threats posed by nonstate actors without state support could be mitigated through deterrence by denial efforts. Positive spillover effects from U.S. active measures against state adversaries could improve defense capabilities against nonstate actors.

[22] Charles Tilly, "War Making and State Making as Organized Crime," in *Bringing the State Back In*, ed. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambridge University Press, 1985).

[23] Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 14, no. 3 (Fall 2019), 122–145.

[24] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012), 5–32, https://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf.

[25] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015), 316–348, https://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cyberspace.pdf.

[26] Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2 (2019), 317–347, https://journals.sagepub.com/doi/full/10.1177/0022002717737138.

[27] Valeriano and Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–2011"; Valeriano, Jensen, and Maness, *Cyber Strategy.*

[28] Claire Metelits, *Inside Insurgency: Violence, Civilians, and Revolutionary Group Behavior* (New York: New York University Press, 2010).

[29] Daniel Byman and Sarah E. Kreps, "Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism," *International Studies Perspectives* 11, no. 1 (2010), 1–18.

[30] William Akoto, "Accountability and Cyber Conflict: Examining Institutional Constraints on the Use of Cyber Proxies," *Conflict Management and Peace Science* 39, no. 3 (2022).

[31] Ibid.

[32] Russell Brandom, "U.S. Institutes New Russia Sanctions in Response to SolarWinds Hack," *The Verge*, April 15, 2021, https://bit.ly/3m7MqM8.

[33] Valeriano, Maness, and Jensen utilize Pearson residuals to compare categorical variables. Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "Cyber War," in *What Do We Know About War?* ed. Sara McLaughlin Mitchell and John A. Vasquez (Lanham, MD: Rowman and Littlefield, 2021), 209–228.

[34] The utility of a state-centric focus in cyber analysis is akin to studying nuclear latency, where a state's organization of resources is a necessary to develop nuclear latent production facilities. See Matthew Fuhrmann and Benjamin Tkach, "Almost Nuclear: Introducing the Nuclear Latency Dataset," *Conflict Management and Peace Science* 32, no. 4 (2015), 443–461. Despite the stated goal of several terrorist organizations to procure or produce nuclear material, only states have successfully undertaken this task. The terrorism literature fails to align with cyber latent capability in one key dimension, however. Cyber entities have acquired sophisticated state-produced capabilities and then turned them against their adversaries. See Farwell and Rohozinski, "Stuxnet and the Future of Cyber Warfare."

[35] Rebecca Slayton, "What Is Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (Winter 2016–2017), 72–109.

[36] Ben Garfinkel and Allan Dafoe, "How Does the Offense-Defense Balance Scale?" *Journal of Strategic Studies* 42, no. 6 (2019), 736–763; Muhammad Mudassar Yamin et al., "Weaponized AI for Cyber Attacks," *Journal of Information Security and Applications* 57 (2021), 1–35.

[37] Gartzke and Lindsay, "Weaving Tangled Webs."

[38] Michael Peck, "The Myth That Bombers Will Always Get Through," *The National Interest*, March 2, 2016, https://nationalinterest.org/feature/the-myth-bombers-will-always-get-through-15369.

[39] Gérard Chaliand, *In the Art of War in World History: From Antiquity to the Nuclear Age* (Berkeley: University of California Press, 1994), 908.

[40] Ibid., 892.

[41] Douhet's influential book, *The Command of Air,* became a foundational text for air power advocates. Douhet argued that once air superiority is attained, mass bombing of military and civilian targets can win wars. Over the decades his theory of air power penetrated numerous countries' air force doctrines. Ultimately, the doctrine of mass targeting of an enemy's civilian infrastructure was outlawed.

[42] Colin Demarest, "Pentagon to Announce Zero-Trust Cyber Strategy," C4ISRNET.com, November 8, 2022, https://www.c4isrnet.com/cyber/2022/11/08/pentagon-to-unveil-zero-trust-cyber-strategy/.

[43] *DoD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, GAO-22-105330 (Washington, DC: Government Accountability Office, 2022), https://www.gao.gov/products/gao-22-105330.

[44] J. Mike McConnell and Mark Grzegorzewski, "Cybersecurity and Strategic Deterrence: Changing Adversary's Risk Versus Reward Calculations," in *The Great Power Competition*, vol. 3, *Cyberspace: The Fifth Domain*, ed. Adib Farhadi, Ronald P. Sanders, and Anthony Masys (Cham, Switzerland: Springer International Publishing, 2022).

[45] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Studies* 7, no. 1 (Spring 2014), 54–67, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1337&context=jss.

[46] Chris Jaikaran, *Cybersecurity: Deterrence Policy*, R74011 (Washington, DC: Congressional Research Service, January 2022), https://crsreports.congress.gov/product/pdf/R/R47011.

[47] Concepts such as persistent engagement elevate the importance of interactions but, nevertheless, undervalue the function of signaling that cyber actions can convey even when the message is garbled (for example, babbling equilibrium). See Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review* (Special Edition 2019), 267–287, https://cyberdefensereview.army.mil/Portals/6/CDR-Special%20Edition-2019_r6.pdf; and Benjamin Edwards et al., "Strategic Aspects of Cyberattack,

Attribution, and Blame," *Proceedings of the National Academy of Science* 114, no. 11 (2017), 2825–2830, https://www.pnas.org/doi/10.1073/pnas.1700442114.

[48] Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization* 70, no. 1 (Winter 2016), 103–131.

[49] Sandeep Baliga et al., "Deterrence With Imperfect Attribution," *American Political Science Review* 114, no. 4 (2020), 1155–1178.

[50] Jonathan Welburn, Justin Grana, and Karen Schwindt, "Cyber Deterrence With Imperfect Attribution and Unverifiable Signaling," *European Journal of Operational Research* 306, no. 3 (May 2023), 1399–1416.

[51] Edwards et al., "Strategic Aspects of Cyberattack, Attribution, and Blame."

[52] Arne Odd Westad, *The Global Cold War* (Cambridge, UK: Cambridge University Press, 2007).

[53] David Kindy, "The Day Soviet Aircraft Attacked American Pilots," *Smithsonian Magazine*, April 9, 2021, https://www.smithsonianmag.com/smithsonian-institution/seventy-years-ago-soviet-mig-15s-attacked-american-pilots-180977440/.

[54] Mark S. Bell and Nicholas L. Miller, "Questioning the Effect of Nuclear Weapons on Conflict," *Journal of Conflict Resolution* 59, no. 1 (2013), 74–92.

[55] Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010), 102–135, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-04_Issue-3/Goodman.pdf.

[56] Erik Gartzke and Jon R. Lindsay, "Introduction: Cross-Domain Deterrence, From Practice to Theory," in Gartzke and Lindsay, *Cross-Domain Deterrence*, 1–24.

[57] Valeriano, Jensen, and Maness, *Cyber Strategy*.

[58] Ibid., 12.

[59] Ryan C. Maness et al., *The Dyadic Cyber Incident and Campaign Dataset, version 2.0*, 2022.

[60] Our coding scheme emphasizes observed attack actions, eliminating the necessity to infer attack intent. This approach is consistent with U.S. classification efforts. For example, when describing cyber activities originating from Russian IP space, U.S. Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly stated that this activity is "not about espionage, it's probably very likely about disruptive or destructive (cyber) activity." See Zachary B. Wolf. "A cyberattack could lead to war. But it is very unlikely," CNN, March 22, 2022. Cyber espionage and information incidents account for 79 percent of Center for Strategic and International Studies data. *Espionage incidents* focus on information-gathering targeting networks, people, technology, and proprietary information. *Criminal incidents* focus on theft for financial gain. *Information incidents* are active cyber actions to interfere with activities (for example, election interference) or access (Web site hacking). *Jamming incidents* are intended to deny information services

(for example, distributed denial-of-service). *Cyber-on-cyber interactions* are also the most common form of interaction, suggesting that cross-domain engagement is still nascent, its developmental trajectory uncertain.

[61] Vipin Narang, "Strategies of Nuclear Proliferation: How States Pursue the Bomb," *International Security* 41, no. 3 (Winter 2016–2017), 110–150.

[62] Michael Horowitz, "The Spread of Nuclear Weapons and International Conflict: Does Experience Matter," *Journal of Conflict Resolution* 53, no. 2 (April 2009), 234–257.

[63] Kyung Suk Lee, James D. Kim, Hwalmin Jin, and Matthew Fuhrmann, "Nuclear Weapons and Low-Level Military Conflict," *International Studies Quarterly* 66, no. 5 (January 2023).

[64] Vipin Narang, "What Does It Take to Deter? Regional Power Postures and International Conflict," *Journal of Conflict Resolution* 57, no. 3 (June 2013), 478–508.

[65] Kinetic response to cyber attacks is very limited, but statements by President Biden clearly indicate that states are thinking about cyber attacks that could lead to kinetic actions. In July 2021, during remarks at the ODNI, Biden made the following statement: "You know, we've seen how cyber threats, including ransomware attacks, increasingly are able to cause damage and disruption to the real world. I can't guarantee this, and you're as informed as I am, but I think it's more likely we're going to end up—well, if we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence. And it's increasing exponentially—the capabilities." See Biden, "Remarks by President Biden at the Office of the Director of National Intelligence."

[66] Michael D. Shear et al., "Strikes on Iran Approved by Trump, Then Abruptly Pulled Back," *New York Times*, June 20, 2019; Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "Cyber War," in *What Do We Know About War?* ed. Sara McLaughlin Mitchell and John A. Vasquez (Lanham, MD: Rowman and Littlefield, 2021), 209–228.

[67] Steve Holland and Matt Spetalnick, "Obama Vows U.S. Response to North Korea Over Sony Cyber Attack," Reuters, December 19, 2014, https://www.reuters.com/article/us-sony-cybersecurity-usa/obama-vows-u-s-response-to-north-korea-over-sony-cyber-attack-idUSKBN0JX1MH20141219.

[68] Christopher Whyte, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy* 35, no. 2 (2016), 93–102.

[69] Monica Kaminska, "Restraint Under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks," *Journal of Cybersecurity* 7, no. 1 (2021), https://academic.oup.com/cybersecurity/article/7/1/tyab008/6162971.

[70] Valeriano, Maness, and Jensen articulate that true deterrence requires that states have the capacity to "forestall an attack in the first place, capabilities to respond, and the credibility to launch retaliatory attacks, and it must also communicate what actions it wants to dissuade." See Valeriano, Maness, and Jensen, "Cyber War," 2021.

[71] Hal W. Brands, *The General vs. the President: MacArthur and Truman at the Brink of Nuclear War* (New York: Doubleday, 2016).

[72] Herb Lin, "President Biden's Policy Changes for Offensive Cyber Operations," *Lawfare*, May 17, 2022, https://www.lawfareblog.com/president-bidens-policy-changes-offensive-cyber-operations.

[73] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978), 167–214.

3

Cumulative Outcomes of Counter–Cyber Operations Campaigns: Contributions to Integrated Deterrence

By J.D. Work

Contemporary strategists have struggled to come to terms with the role of cyber operations in deterrence. Starting from the earliest missions, grounded entirely in the complex and deeply considered problems of nuclear capabilities, attempts have been made to fit new strategic exchanges into prior logics of punishment and denial. To the extent that the operational objectives involved countervalue and even counterforce strategies, adaptations of classic deterrence logics offered at least a superficially satisficing although awkward fit. However, over the course of decades of adversary capabilities development and employment, it became clear that the ultimate flaws in this understanding had been elided by the limitations of analogy. As a result, a new strategic vision was needed, leading to the emergence of new theory.[1] At the same time, deterrence remains the foundation of U.S. military purpose. How then does the Department of Defense (DOD), U.S. Cyber Command (USCYBERCOM), and the other cyber operations elements of the U.S. Government (and its allies and partners) square what seems to be an impossible circle?

This paper proposes a new conceptual contribution which recognizes the actual nature of cyber engagements "on the wire." It seeks to describe the novel characteristics of both the domain and the engagements that occur within it. These necessarily change the dynamics of deterrence in unique ways. It explores the outcomes that arise from constant contact. Here, cyber capabilities are in continuous use within highly iterated, predominantly silent duels between nth party participants for intelligence, positional, and direct-action objectives under fundamentally different technical and operational conditions than in prior conventional or nuclear contests. It further identifies new emphasis on a previously little-considered variable in the calculus of strategic exchange and outlines new structural interactions that contribute to deterrence outcomes across the cumulative weight of cyber campaigns, with a focus on counter–cyber operations. Recognition of these ongoing dynamics will offer insights to better support future operations planning, tailor effects, and synchronize with other instruments of national power, which in turn will ultimately alter adversary perceptions of credibility, (im)plausible deniability, and associated decisionmaking resolve.

Counter–cyber operations (CCO) actively seek to deny, degrade, disrupt, deceive, and destroy adversary offensive cyber capabilities. These operations serve to defeat adversary access, deny an adversary freedom of maneuver, and defeat positional advantage. During execution against these objectives, counter–cyber operations will remove specific capabilities from the adversary's future options space, and as viable portfolios in their arsenal. In game theoretic analogy, this may "unload the gun" held by the adversary in a duel—and due to the unique nature of the domain and its capabilities, may do so silently (without the adversary's awareness). Counter–cyber operations—including the subset of defensive cyber operations response actions—are conducted against deployed instances of adversary capabilities and/or supporting command and control (C2) infrastructure. CCO must be distinguished from offensive cyber operations for counterforce targeting of an adversary cyber forces, which are directed against military and intelligence services and associated contractor or mercenary organizations to degrade tooling develop-

ment, infrastructure acquisition, and other force generation functions (intended in common analogy to "kill the archer").[2] This distinction arises out of the fundamentally different qualities of offensive cyber arsenals compared to nuclear forces, and may be observed in various unique targeting courses of action. The ability to repeatedly replicate tooling and tradecraft in the context of new accesses requires that countering actions against instantiations of a given capability, which create effects within variable (often transitory) scope across time and differing kill chains, must be considered separately from engagement of the forces that generate and sustain these capabilities.

Beyond immediate operational objectives, it is important to recognize that the value of counter–cyber engagements arises from the weight of cumulative effect. Engagement must be through sustained time and investment, pursued through campaigns consisting of a sequence of operational lines of effort of sufficient scale, concurrency, scope, and duration consistent to match (and overmatch) a given adversary's postured strategic offensive cyber capabilities. The centrality of campaigning in the cyber domain has already been well recognized by cyber persistence theory.[3] The unique technical and operational features of these engagements also create new dynamics in the interaction between defenders and adversaries, that provide the potential for novel contributions toward integrated deterrence objectives.

The cumulative outcome of counter–cyber campaigns may erode adversary offensive capabilities, blunting potential effects that may be delivered against targets held at risk by these objectives, in ways that had not been possible within the kinetic domains. The erosion of these capabilities may change the opposition's perception of relative benefits from aggression relative to restraint in the decision to employ offensive cyber effects at strategic thresholds, causing them to discount payoffs from future aggression (and potentially thereby instead choosing a course of action of restraint).

These interactions must be recognized as fundamentally representing a new causal mechanism of deterrence by erosion of capability, and as distinct from strategies of deterrence by punishment (and retaliation), deterrence by denial, deterrence by norms (or taboos), or deterrence by entanglement. This

mechanism for erosion was notably first outlined in the nuclear deterrence context by Barry Posen over three decades ago, but then considered only as a potential driver of escalation (as will be discussed in detail below).[4] I reconceptualize these interactions within the cyber domain based on the unique character of counter–cyber options, and further examine the effects from erosion of capabilities toward corroding credibility of adversary coercive threats, as well as creating further potential impacts on resolve. I identify deterrence by erosion of capability as a higher order objective for counter–cyber operations campaigning. Such campaigning has impact both from resetting conditions of security and insecurity at the operational level and thereby redefining the facts "on the wire" (as described by cyber persistence theory), but also where the cumulative effects of appropriately scoped and sequenced operations introduce key uncertainty for adversary decisionmakers. This uncertainty changes the calculus of risks versus potential gains for actions involving offensive cyber effects at or above strategic thresholds of conflict.

This latter dynamic does diverge from cyber persistence theory's assertion that deterrence is not viable within the cyber domain, as states will always have an imperative to act and to persist in their courses of action.[5] Here, I concur that prior mechanisms of deterrence did not alter this imperative, especially for interactions below the threshold across dimensions of competition and subcrisis maneuvering. However, the novel opportunities afforded by erosion of capability may change these interactions, especially on the cusp of conflict and in the course of ongoing attack exchanges. There is strong explanatory value in understanding the structural imperative pressures on states to find and exploit vulnerabilities for their own power advantages toward realizing gains in and through the cyber domain, which in turn limits (or as may be argued, precludes entirely) the circumstances under which a defender's actions may alter this strategic calculus.[6] However, conditions in which the adversary's appreciation of potential payoffs from aggressive courses of action may be discounted can be shown to, and will likely occur, in a range of potential conflict interactions resulting from the mechanism of erosion of capability. This points to scenarios under which deterrence outcomes may

influence specific adversary decisions, within the context of a given crisis, and influencing prospective strategic cyber "fires," even as wider structural pressures will continue to drive repeated iterations of this contest.

To advance its overall thesis, the paper proceeds as follows: The first and second section reviews the current state of deterrence theory in its nuclear and conventional forces applications and outlines the ever-hardening positions within debates over the extension of this theory to the cyber domain. I then turn in the third section to consider cyber operations contributions to integrated deterrence, broken down into seven parts.

I start from first principles to account for the unique features of the domain and the fundamental differences in character and results of strategic exchanges involving offensive cyber operations in the original mission of exquisite nuclear counterforce targeting. From this recently declassified history, we identify the causal mechanism of capability erosion inherent in this mission and reconceptualize these outcomes as potential contributions toward integrated deterrence vice merely an escalatory risk (as they were considered under conditions of strategic nuclear stability). I then explore these interactions beyond the nuclear domain, within the context of strategic offensive cyber effects capabilities intended to substitute for nuclear fires. Critical distinctions are introduced that must be made between CCO and offensive cyber operations for counterforce targeting of adversary cyber forces, and briefly note case examples that suggest that the latter such options offer limited utility for deterrence. I proceed with in-depth exploration of CCO intended to erode an adversary's strategic offensive cyber effects capabilities, noting the extended scope and duration of these interactions in comparison to traditional conceptions of nuclear exchange, and the hider-finder dynamics inherent in these contests across gray and red cyberspace distinct from mistaken analogies of a cyber "commons." The various objectives of CCO are explored, looking at ways to "silently unload" the adversary's gun, and their potential to discount adversary payoffs for aggression via the delivery of strategic cyber fires. I further consider these in the context of concurrent defensive cyber operations and review the impact of increasing attacker costs

for actions against hardened targets, as well as noting the parallel and distinct interactions of counterintelligence operational games. I finish the section by mapping perceptions of discounted payoffs created by the erosion of capability across the dimensions by which this may result in the corrosion of credibility, noting the key role of the introduction of uncertainty in the net assessment of relative capability, and further considering the implications of sunk costs, variability of adversary resolve, and what ultimately arises once again as the central question of estimating adversary intentions.

I conclude the paper by summarizing the rediscovered mechanism of deterrence by erosion of capability as only one part of a wider equation of restraint and aggression, bound at the upper threshold by the nuclear umbrella, highlighting the critical importance of initiative and intelligence in these interactions, and laying out further research questions intended to validate and extend understanding of these dynamics.

Deterrence Theory in Nuclear and Conventional Domains

There are few areas of study in international relations with deeper literature than theories of deterrence. From initial conceptions to contemporary operational practice, there is not only a well-validated canon over the decades of superpower nuclear contests, but also myriad specialist explorations across crisis histories, applications beyond nuclear warfighting, and efforts to grapple with changing actors and their interactions. Full exegesis of the inception, debates, and evolution of this thinking across the multiple waves of the field, and its modern reinterpretations, is beyond the scope of this present work.[7] However, one builds on the foundation laid by so many earlier scholars. The vital underpinnings of that foundation in this analysis are in the recognition of distinctions within the fundamental mechanisms by which deterrence is accomplished: by punishment (including retaliation) and by denial (including options preventing battlefield success and via reduction of vulnerability to threats).[8] Although this does not discount more contemporary ideas that have stretched the concepts of deterrence, including mechanisms of deterrence by entanglement and through the influence of overarching norms or

taboos, these ideas factor less heavily in the present analysis.[9] All of these concepts recognize the centrality of coercive processes that alter an adversary's cost-benefit calculus, changing strategic decision choices.[10] Critical distinctions must nonetheless be made in any analysis of how deterrence mechanisms are operationalized, and create effects, in differing strategic domains, from nuclear, to conventional, and beyond.[11]

In taking stock of deterrence in the post–Cold War period, the question of credibility has risen to the forefront—and remains so for this analysis. Although credibility has generally been seen as an irreducible factor for deterrence, it was often relegated to the "difficult and delicate" realm of intentions.[12] Unpacking intentions for outcomes of mutually assured destruction even led to questioning the rationality (or irrationality) involved in the pursuit of such courses of action.[13] Yet much of the scholarship around these more intangible factors would emerge only when the more concrete observables of arsenal sizing and force design, deployment, and concepts of operation were seen as solved. At the same time, the wider questions of purpose and utility in a changing international landscape became newly unsettled as world order demonstrably changed. The assumptions of earlier Great Power competition across multiple instruments of national power had held that every interaction potentially affected adversary views of commitment, and that "losing" in the calculus of relative exchange in diplomatic, economic, or conventional military contexts short of war would undermine strategic deterrence. This interdependence was seen to arise from political psychology, influenced by factors of leadership perception, as much as the operational state of any given deterrent capability set.[14] More recent thinking has distinguished the factors of reputation, and found that decisionmakers focus more on the capability to hold targets at risk, and operations to execute on that threat within the context of a crisis.[15] This reasoning apparently holds true, particularly across repeated interactions in which the variable stakes and differing outcomes of disputes between states complicate perceptions—although critically, reputation likely factors more heavily in general deterrence beyond specific crisis

events.[16] The cumulative nature of these interactions thus also emerges as key when considering new decisionmakers in asymmetric hostilities.[17]

Most efforts to understand these important questions of perceptions of commitment, resolve, and reputation across iterated interactions are, however, grounded on previous operational realities in different strategic domains. In these earlier contexts, once established, the capability to threaten was an unalterable fact. Thus, factors of political psychology determining how these threats were perceived became the critical variables of credibility. Such dynamics nonetheless change when considering operations in and through the cyber domain, where operational realities may render capabilities more ephemeral.

Cyber Deterrence Literature and Its Discontents

The adaptation of deterrence theory to the new warfighting and strategic domain of cyberspace has itself spawned innumerable works. These efforts originate both from scholars versed in classic ideas and who have sought to reflect upon the manner in which these concepts might be extended, as well as practitioners who have been forced by circumstance to engage with strategy and policy in various ways (albeit not always consistent with a full scope of the underlying academic research). Senior academics, and many newer entrants who follow in their example, have grappled with explaining the canonical pillars of deterrence theory in light of this new environment.[18] Differing interpretations have also been advanced which encompass deterring adversary actions in cyberspace, through both in domain and cross-domain means, as well as the use of cyber itself as a tool to deter actions in differing environments. Useful approaches have been advanced to conceptualize differing cross-domain deterrence dynamics.[19] Various works have focused on the viability of retaliatory threats in the face of a more complex attribution landscape (erroneously often stated in theory as impractical or otherwise beyond reach, despite mounting evidence of attribution in practice).[20] Some effort has been made to understand unique features of the credibility of threats communicated in the domain as a core pillar of coercive outcomes, including

the relative costliness of various operations as means of signaling.[21] Recent efforts have sought to focus on the potential specific extension of deterrence by denial, including through vulnerability reduction unique to technical problems in the domain, or via various forms of active defense.[22] Such work itself builds on and subsequently informs the wider questions around the potential contestability of offensive cyber operations and their effects, and the resulting implications for offense—defense balance.[23] Iterated success in contesting potential adversary cyber action through both intelligence and one's own offensive capabilities has further been recognized as a critical element of strategic interactions toward deterrence of threats.[24]

The utility of this theoretic extension of deterrence scholarship remains contested. A useful effort has been made to map large conceptual trends in the literature to reflections in state practice.[25] Yet several years ago, the volume and often repetitive quality of writings seeking to extend deterrence theory to encompass cyber operations reached the point that a group of academics, practitioners, and policymakers surveying the state of the field declared the subject "uninteresting" for further time and attention.[26] Nonetheless, demand signal from decisionmakers facing the problems of the domain has continued unabated.

As a matter of day-to-day operations, practitioners on the front lines (and the scholars who have worked with them) observe substantial indications that adversary behavior remains unchanged by the prospect of punishment in retaliation for intrusion or even destructive effects.[27] This reality has even led to major private sector firms declaring their own deterrence approaches, implicitly suggesting that state practices alone are insufficient and that the power within the cyber domain that may be leveraged by private actors is required to reinforce deterrence approaches, to whatever extent they (mis) understand and align actions with theory.[28] Although these conditions may change when one considers actions that might fall above the threshold of armed conflict, a growing consensus is emerging among those professionals tasked with evaluating threat intentions that deterrence does not operate as a mechanism of Great Power competition, at least where encompassing es-

pionage, crime, and potentially covert action.[29] New research has also sought to test this consensus, and to provide analytic rigor to clarify expectations of deterrence outcomes, as well as in evaluating deterrence success or failure in the domain.[30]

The prospect of deterrence by denial via vulnerability reduction—reducing the payoff for exploitation of targeted systems and networks by eliminating opportunities to compromise through hardening—likewise seems dim. Although this hope is attractive in theory, where the secure development principle that "many eyes make all bugs shallow," would seem to offer promise is that at some sufficient threshold of investment in both cornering the market on new bugs and patching against new bugs, it would tip deterrence equations against the challenger.[31] However, recurring vulnerability discovery across even heavily targeted attack surfaces continues to yield new exploit options.[32] The number of attack surfaces of interest also continues to rise exponentially given the constant introduction of new systems, services, and functions in the "small pieces, loosely joined" model that serves as the fundamental value creation mechanism of the domain.[33] These relationships of scale, complexity, and value lead inexorably to the failure of vulnerability reduction in present ecosystems.[34] Payoffs for adversary exploitation, therefore, are not substantively altered.

Scholars working with DOD and USCYBERCOM have also advanced a new theory that offers alternative explanations for strategic dynamics and interactions within the domain. Cyber persistence theory reaches beyond deterrence to consider fundamental conditions "on the wire," where cyber forces are not held in reserve but are in "constant contact," leading to a contest of initiative defined by setting and resetting conditions of security shaped by systems and networks that remain vulnerable to exploitation.[35] Other researchers have also focused on the element of initiative, proposing mechanisms of deterrence arising out of surprise, operationalized through engagement via the instruments of intelligence and influence operations.[36] Alternative explanations that describe cyber operations as an intelligence contest, rather than a contest of arms or initiative, have also been advanced.[37]

These include efforts to recast cyber operations within analytic frames used for mechanisms of subversion or covert action.[38]

Debate between deterrence theory and alternative explanations for strategic behaviors was also taken up by the U.S. Government's Cyberspace Solarium Commission, in an effort intended to evaluate competing strategic theory in the domain.[39] The effort was deliberately modeled on the Eisenhower-era Solarium, which shaped policy for the early Cold War.[40] Unfortunately, the competitive testing approach was not followed through and the resulting recommendations were issued encompassing "all of the above" selections across diametrically opposed policy options, prompting some participants to note that this rendered the commission a failure under its terms of reference.[41]

Thus, the study of deterrence in cyberspace must still confront what remains an unresolved debate. As in any subfield, multiple directions of change in the literature to come may be anticipated—and some scholars have offered thoughts toward this end.[42] However, despite the need to come to terms with these concepts, there is increasingly little appetite for such conversations given the daunting scope of prior works that must be addressed and limited academic incentives for publication on what is perceived as well-trod ground. This task is compounded by what many perceive as a too frequently toxic climate in review, especially for journals focused on cyber specific subjects.[43]

Cyberspace Operations and Integrated Deterrence

The recurring attempts to address how cyberspace operations fit into deterrence theory are not merely an academic fashion, nor simply a case of new practitioners stumbling onto old theories and trying to leverage them ad hoc for mission or budgetary justifications. U.S. national security strategy, and associated national defense strategy, is inescapably grounded in the policy choices of deterrence. National strategies also continue to evolve the approach that the U.S. Government will pursue to achieve deterrence outcomes—including tailored deterrence, and now newer integrated deterrence concepts.[44] Although alternative ideas such as cyber persistence theory may

offer greater explanatory value for analysis, and the prospect of improved futures estimates, there is still a need to explore the relationships between the conduct of cyber operations (even if they are conducted according to their own unique logics) and integration of these operations into larger national strategies anchored on altering adversary cost-benefit calculus.

This may seem a daunting task, if not an attempt to square an impossible circle. Given seemingly inevitable recurring cycles of effort, it is certainly frustrating for scholars and practitioners that are repeatedly called on to address the question.[45] Yet prior evaluation of deterrence theory for the cyber domain has often suffered at several levels: by failing to address unique structural features of the domain; by failing to evaluate the specific interactions arising from and shaped by those unique structural features; by abstracting too broadly what are key technical details at the operational level or distorting the strategic picture through flawed analogy and/or oversimplification; by failing to account for significant missions, major case incidents, and the associated evolution of capabilities due to the opacity of the domain (which arises out of classification and other nondisclosure limitations); or in failing to fully assess the volume/variety/velocity of interactions.

These issues have elided fundamental differences in the character and results of strategic exchanges in and through cyberspace with substantial implications for deterrent outcomes. To understand these dynamics requires we return to reexamine strategic "cyber fires" from first principles.

Offensive Cyber Operations in the First Strategic Mission

In part, prior understandings of cyber operations have been distorted by their unique origin as a heavily classified capability. The full details of this inception as yet remain unclear, however recent declassification has resulted in disclosure of key historical programs, without which it was previously nearly impossible to understand the strategic mission for offensive cyber programs. (Although public recognition of the potential for this mission does date to the earliest conceptions of offensive malware and the popularization of the

term *cyberspace*.[46]) This new disclosure also changes how we may understand the contributions of cyber capabilities toward deterrence.

Offensive cyber capabilities have been described as the first military innovation to arise from the intelligence community. The first objective to which this innovation was directed is now known to be options intended to defeat nuclear command and control targets. Under President Ronald Reagan, and the program's early founders, this was explicitly conceived of as a damage limitation measure, an effort to preserve U.S. cities and population should the worst-case scenarios of a nuclear exchange come to pass.[47] Although details of this capability and its evolution over time remain limited, a number of scholars have explored the potential targeting of nuclear forces through "new" cyber means even in the absence of knowledge of their prior development, creating an extensive unclassified literature through which such operations may be considered.[48] These have included efforts to wargame cyber and nuclear interactions at various levels of detail and fidelity.[49]

Treating offensive cyber options in "left of launch" engagements as damage limitation, under either preemptive or as execute-on-warning mission models, has tended to mean these capabilities are considered in an already familiar strategic calculus. Damage limitation approaches are by no means without their own controversies, and the debates over the degree to which such strategic posture may alter deterrence calculus, or potentially degrade nuclear stability, have been extensive and illuminating.[50] Where offensive cyber is merely conceptualized as a means of stopping incoming missiles in exchange scenarios, and thus relegated to consideration as something like missile defense, this is however somewhat distorting. Rather, offensive cyber options delivered effects against adversary nuclear command, control, and communications (NC3) are arguably better thought of as an exquisite counterforce capability. Some scholars have thus far recognized these dynamics and sought to explore the implications as these capabilities become more widely understood by adversary planners.[51]

This variable awareness poses its own difficulties in assessing the value of cyber capabilities for deterrence outcomes. An adversary that is not aware

of these options, and their potential to alter the payoff in the decision to attack, is unlikely to be deterred. This difficulty is not an issue unique to cyber operations. The challenge of assessing the impact of clandestine capabilities on deterrence has been acknowledged as a central problem in current theory, and for its operational implications.[52] It has sparked questions about timing and value of selective disclosure to achieve political gains.[53] Offensive cyber capabilities also impose unique difficulties in acknowledging potential effects without revealing the vulnerabilities that may be exploited to achieve these options, so as to avoid adversary defensive mitigation which would nullify or defeat the capability.[54] These challenges also inform fundamental features of operational planning, where decisions to leverage a given vulnerability or to hold in reserve become critical in both immediate exchanges and over the course of iterated contests.[55] Recent cases have suggested that the density of vulnerabilities across a variety of potential system and network targets remains sufficient to allow for some degree of signaling—as has been likely observed in the "bugs on parade" at vulnerability disclosure competitions such as China's Tianfu Cup.[56] However, such bug density may not extend beyond commercial, enterprise, and consumer technologies to unique strategic targets such as NC3 or other critical military systems.

Indeed, it is likely that Soviet leadership became aware of novel Western capabilities to target NC3 during the Cold War, at least in part via espionage successes delivered by the East German Ministry for State Security (Ministerium für Staatssicherheit) Main Directorate for Reconnaissance (Hauptverwaltung A) penetration of associated U.S. field activities conducted under the CANOPY WING program.[57] One may presume that other states have been aware of the potential, if not also the details, of such nuclear counterforce options since that period. There is indeed some (albeit limited) evidence in the open source to validate this inference. In April 2019, People's Liberation Army Senior Colonel Weidi Xu publicly objected to potential use of militarized cyber capabilities in "left of launch" operations against nuclear forces, saying these sent "a dangerous signal." These remarks were directed specifically as challenges to several current and former senior intelligence officers

acknowledged to focus on the cyber portfolio.[58] Similar concerns highlighting concerns regarding risks to nuclear strategic stability have been raised in formal journal publications.[59]

Reconceptualizing Mechanisms of Deterrence by Erosion of Capability

However, treating the novel innovation of offensive cyber options as counterforce in the same model as kinetic (nuclear or conventional) fires against adversary strategic systems elides the unique character of the capability. Offensive cyber capabilities are exquisite in their ability to erode adversary warfighting capability without directly crossing thresholds involved in kinetic weapons employment. In game theoretic analogy, offensive cyber operations may "unload the gun" (for example, silo or launcher) of an adversary in a duel. Even in the most basic of effects delivery that is denial of service, these effects remove a specific platform from the adversary's standing arsenal and/or its deployed posture. Such removal functions in the least instance for some given period of time, if not as a permanent "functional kill," as the effects of an offensive cyber capability are transitory across a variable temporal scope that are defined by the "fast equations" that dictate weaponeering and arsenal management decisions.[60] This option is unique among other warfighting courses of action, as the prospect to do so remotely, at scale, and at the speed of an imminent exchange of nuclear fires is provided by no other capability disclosed to date. In earlier eras, the erosion of strategic capabilities without attack occurred only via friction, or failure by chance.

Erosion of capability in turn leads to uncertainty regarding technical reliability and operational availability, as well as uncertainty in potential effects delivery. This uncertainty exacerbates the unknowns that are at the heart of so many potential cyber attack and exploitation plans, which involve constantly shifting target environments, changing technology stacks, and variables of chance and even luck. This uncertainty effectively corrodes the credibility of a targeted strategic option for both an adversary's leadership, as well as other parties that may be aware of the degraded state of the capability.

The awareness that a capability may not reliably be counted on to perform when called on, especially under crisis pressures, thus alters payoffs from prospective courses of action. (It remains exceptionally important to understand the differences in behaviors between crisis and noncrisis interactions, which scholars have noted continues to confound less informed debate.[61])

Although the potential to erode adversary capability (and corrode credibility) has previously been recognized as a consequence of counterforce and damage limitation strategies through other nonnuclear capabilities targeting nuclear forces, it was relegated to examination as a negative outcome. First and most seriously, this was seen as a potential driver for inadvertent escalation. Where such actions at sufficient scale may undermine an adversary's assurance that they may successfully employ a reserved retaliatory capability, threatened states may respond through measures that raise the risk of prompt use. [62] This is, of course, consistent with long-standing analysis which finds that first-strike incentives created by nuclear counterforce options have are particularly problematic for nuclear stability.[63] The potential for inadvertent escalation arising from contesting nuclear delivery specifically using cyber capabilities has also been further explored.[64] These potentials arise as variants of dilemmas created by other conventional counterforce options.[65] Beyond specific escalatory interactions, the fact of the potential for covert or clandestine degradation of nuclear forces may undermine key information symmetries that are critical for deterrence stability.[66]

Across these scenarios, familiar problems are encountered in which potential preemptive concepts of operations exacerbate first-strike incentives. At the same time, a more restrained execute-on-warning mission model places exceptional requirements on a state's intelligence service: to provide appropriate visibility into adversary launch preparations within what are now very compressed timelines for contemporary strategic weapons systems and to ensure that indications of imminent attack are appropriately assessed and communicated clearly. These requirements must also be met within a sufficient advance window to allow cyber forces to act before potential loss of options. These options are in part perishable due to changing communications se-

curity, network maneuver, or other conditions that will arise as an adversary force shifts its posture across the spectrum from research and development testing, to deployed deterrence missions, to limited fires involving similar strategic delivery systems employed in conventional kinetic effects roles, to actively fighting a nuclear exchange.[67]

Nuclear planners also recognized the potential for erosion of capability as a result of ordinary friction and failure in nuclear arsenals, particularly following the imposition of treaty prohibitions on nuclear testing. The creeping uncertainties that were introduced by aging nuclear warhead inventories, or new designs that had never been tested "end to end" (to backport the vernacular of the cyber domain), were deemed unacceptable. Efforts were required to avoid the perception of corroded credibility where such uncertainties may have been presumed to exist. As a result, the U.S. Government invested extensively in its Stockpile Stewardship Program.[68] This includes the very prominent and cutting-edge assurance options afforded by the National Ignition Facility, whose public research outputs provided a proxy to demonstrate the ability to conduct robust analysis within very unique high energy density physics regimes.[69] This is both a costly signal as well as a form of signaling that offers a high degree of technical fidelity that would be otherwise difficult if not impossible to replicate. This speaks to the importance U.S. planners have attached to avoiding even the perception uncertainty that might undermine nuclear domain capabilities.

It is natural to treat erosion of capability in a nuclear warfighting domain as a concern, especially where it may threaten strategic stability or place additional "use or lose" pressures on adversary decisionmakers in crisis. Uncertainty created by erosion of capability that in turn corrodes credibility of nuclear deterrence forces indeed has the potential to introduce a brittleness in decisionmaking, where leaders may reject other flexible options in crisis for fear of loss of positive control over nuclear forces. The limited declassification of only a narrowly scope of a specific historical period also raises questions of whether uncertainty may even in practice arise in the nuclear domain on the basis of cyber interactions given modernization of NC3 in its contemporary

incarnation. This is perhaps a good thing given the concerns raised regarding the potential impact to deterrence stability. Yet focusing solely on these negative outcomes has overlooked the potential mechanisms by which such erosion may contribute to deterrence outside of the nuclear strategic domain, given the unique character of cyber operations interactions.

Strategic Offensive Cyber Effects Capabilities in Other Than Nuclear Contests

Beyond the first mission of offensive cyber as an exquisite nuclear counterforce option, extant programs have been developed to pursue "lesser included" missions for strategic effects delivery as a substitute for nuclear or other kinetic capabilities. These options have been deliberately conceptualized as an alternative to conventional warfighting, and as a tool that may be employed at different phases of a militarized crisis or during ongoing conflict for varying reasons of escalation avoidance, ability to service targets at lower risk to other forces, or unique enabling functions intended to shape contact between forces.[70] The various concepts of operation for strategic effects employment, and associated doctrines that have been developed by U.S. and allied forces, and their strategic competitors, have been widely discussed in literature, although they are still too often poorly understood in their evolution over the decades.[71]

Offensive cyber operations may support strategies of deterrence by punishment (including as retaliation) when employed to directly target adversary critical infrastructure and key resources. Such mechanisms of direct cost imposition are explicitly discussed within unclassified U.S. national defense strategy.[72] Strategic effects delivery through cyber operations, however, requires more than what is commonly envisioned as a single encapsulated crisis moment of fires exchange as in the nuclear domain (whether that "moment" is measured in minutes of intercontinental ballistic missile launch until impact, or hours of bomber flight to weapon release). For effective cyber fires, an adversary must pursue measures for operational preparation of the environment to ensure access and the ability to degrade or destroy critical

processes, in turn leveraging well-tailored intelligence regarding the target systems and networks. There has been robust evidence of ongoing efforts by multiple states to pursue such capabilities, and exercise as practice—if not pre-position for future crisis—various operational preparation of the environment measures.[73] These actions form part of the backdrop of "constant contact" in the domain, where cyber forces are characterized not by readiness in reserve but by ongoing use.[74] Such constant contact gives rise to unique dynamics that have only been partially explored to date. Scholars have considered the escalatory potential inherent in these interactions, especially given the difficulty in distinguishing such destructive preparations from "mere espionage" intended only to steal information through compromise of system confidentiality.[75]

These actions occur over time, in variable sequences of vulnerability discovery, exploitation, access, and spiral development of implants that can deliver variable effects across differing systems and network targets. To reach strategic thresholds, they must when called on to service a wide number of such possible targets, especially when considering use as strategic substitution for other countervalue targeting options. These extend not only across the geographic considerations that would be familiar to nuclear targeteers, but also across the 17+ critical infrastructure and key resource sectors that make up the essential functions of the economy.[76] A full enumeration of comparative "designated ground zero" equivalents is beyond the scope of this paper, however such analysis almost certainly yields a number of target nodes easily equivalent to nuclear strategic problems, even assuming for simplification purposes a mere duopoly among firms providing services in each of the relevant critical infrastructure sectors (which, of course, is rarely the case in actual markets that see robust competition by many firms). Unlike the ability to designate each nuclear strategic target to be serviced by any of a few broad classes of warheads, cyber effects often demand uniquely developed offensive options for each target, or at least tailored across some curve of common technology solutions, and adoption across industries further complicates this targeting picture. Although concentration effects of cloud business models

and other highly successful offerings that focus on hyperscale customer aggregation may allow some similar scaling of offensive reach, even these present their own exponential problems of independent service and regional architectures.

In short, a viable strategic capability requires sustained time and investment, pursued through a sequence of operational lines of effort of sufficient scale, concurrency, scope, and duration. The campaign is therefore the proper unit of analysis in evaluating comparative strategic capabilities.[77] These campaigns hinge on requirements for the successful initial intelligence and reconnaissance to support development of tailored effects capabilities, as well as operational preparation of the environment required to support posturing and, in some cases, pre-positioning these capabilities through such sustained campaigns. These campaign requirements, when recognized as dependencies, create novel potential opportunity for defenders to contest offensive cyber strategic delivery options.

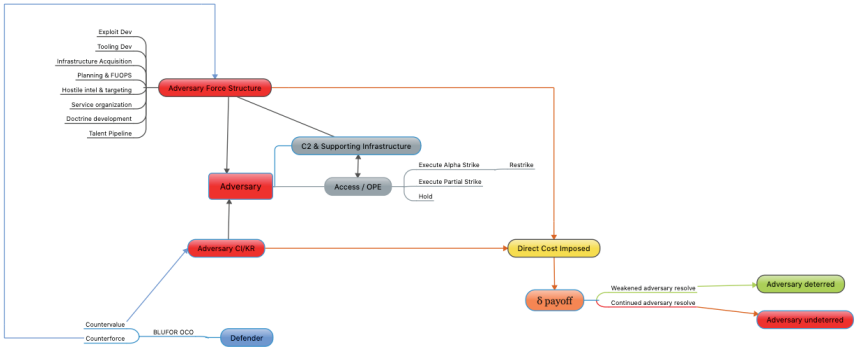
It should further be noted that the uncertainties inherent in these requirements will often lead decisionmakers to favor the better understood modalities of kinetic offense. There remains a perceived degree of reliability, and of finality, in the delivery of conventional fires through platforms that have been in long use, with lineages in military operations stretching back hundreds of years. Yet under a variety of scenarios—one may consider the substitution of cyber effects or kinetic fires on an interchangeable basis—there are a variety of circumstances that may make the reach, scale, speed, reversibility, or target specific dependency factors of offensive cyber operations particularly advantageous. Here, planners are likely more inclined to thus accept and address unique campaign requirements needed to support offensive cyber as an exquisite, or at least more rarified, implement of effect over more readily understood high explosive or directed energy options. In these cases, the opportunities to contest the way the opposition pursues these requirements may itself tip the balance of substitution decisions back toward conventional kinetic fires, stripping these advantages and potentially changing perceptions of payoff in the absence of some factors that may have made

aggression executed in and through cyberspace less costly (for example, non-attribution and the absence of high visibility artifacts of violence for media coverage, among others).

Offensive Cyber Operations for Counterforce Targeting of Adversary Cyber Forces

In common game theoretic analogy, counterforce operations "kill the archer"—seeking to halt offensive effects delivery and execution on target. Where executed through cyber attack, counterforce against an adversary's strategic cyber forces may destroy or degrade exploit and tooling development, infrastructure acquisition, planning for current and future operations, as well as the functions of the military and/or intelligence service organizations that man, train, equip, and direct these forces. These operations should be distinguished from counter–cyber operations (including the subset of activities defined in U.S. doctrine as defensive cyber operations response actions), which seek to exploit and degrade/destroy/disrupt an adversary's

Figure 1. Deterrence Interactions from Offensive Cyber Operations Employed for Strategic Countervalue and Counterforce Targeting



deployed offensive accesses, implants, C2, and associated operational infrastructure.[78] Counterforce options may contribute to integrated deterrence by altering the adversary's calculation payoff for its ongoing or prospective offensive actions through direct cost imposition.

However, there is little evidence that deterrent outcomes have resulted in the few cases where counterforce operations against adversary cyber force structure have been publicly observed. The contribution of offensive cyber counterforce operations, which reportedly degraded contractor entities supporting Russian government–directed influence operations campaigns, including tooling and task organization supporting coordinated inauthentic behavior in advance of the 2018 U.S. Federal midterm elections, were likely intended to contribute to deterrent outcomes across multiple political seasons.[79] Yet renewed adversary malign influence behavior was observed by commercial intelligence services in advance of the 2020 U.S. Federal elections, along with additional activity that may be characterized as initial reconnaissance in small scale intrusion against peripheral polling related networks in September 2020. This activity halted, however, following bilateral meetings between high-level U.S. and Russian national security officials, suggesting that intelligence diplomacy played more of a role in deterring adversary action in that cycle than earlier counterforce operations. Nonetheless, the credibility of backchannel diplomatic overtures may have been well established by these earlier campaigns, along with concurrent counter–cyber operations against other Russian nexus threat actors conducted during those months.[80]

Between April 2010 and at least February 2016, sustained campaigns of disruptive distributed denial of service cyber attacks were attributed to the government of the Islamic Republic of Iran. During September and October 2012, likely retaliatory counterforce offensive cyber operations were observed being conducted by unknown parties against elements of the Iranian government.[81] These engagements did not appear to materially alter adversary behavior, and presumably associated decisionmaking, during the further course of the campaign. Stronger evidence suggests that CCO direct-

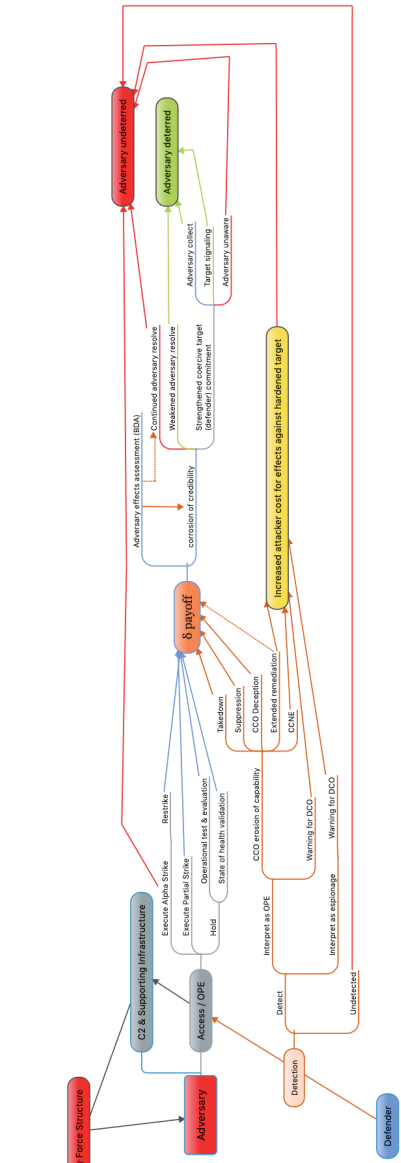
ed against deployed adversary botnet C2 and associated server infrastructure in January 2013, and again in July–August 2013, were likely more salient.[82]

In a more difficult case, a combination of offensive cyber operations employed for counterforce objectives against Iranian nexus cyber forces, and CCO against Iranian attributed cyber espionage infrastructure supporting Islamic Revolutionary Guard Corps irregular kinetic naval operations in the Persian Gulf, were conducted by unknown parties in the summer of 2019. This campaign does appear to have had some impact on adversary decision-making, and may have changed the potential calculus for leveraging then wider regional compromises across energy, water, telecom, and maritime transportation targets in retaliatory actions employing destructive cyber effects during a militarized crisis.[83] Yet disentangling what element of the as yet still unclear scope and effects of operations offered which contributions toward deterring further immediate cycles of Iranian aggression remains challenging, and will likely require waiting for a more complete review at appropriate historical interval.

Erosion of Strategic Offensive Cyber Effects Capabilities Through Counter–Cyber Operations

The unique technical characteristics of capabilities required to conduct credible offensive cyber effects operations create options to respond to adversary campaigns beyond counterforce targeting. Because these interactions are not the traditionally conceived "missiles in silos" of the nuclear domain, but rather a more complex mix of presence, opportunity, and asymmetrical information, these options are not generally encompassed within single event or incident engagements. Rather, they must be addressed through persistent campaigning employing offensive capabilities for counter–cyber objectives. The cumulative outcome of counter–cyber campaigns may erode adversary offensive capabilities posture, undermining aggregate strategic value of accesses, deployed malicious implants, and ongoing C2. Counter–cyber operations may blunt the effects that can be delivered within target systems and networks held at risk by these intrusion footholds, changing outcomes both

Figure 2. Deterrence Interactions from Counter–Cyber Operations to Erode Adversary Offensive Cyber Effects Capabilities



for specific objectives and in wider appreciation across critical sectors and geographies. The variable ways and means by which such erosion is achieved, and the adversary's differential awareness of these losses, will alter the opposition's perception of payoff for aggression and thereby contribute to deterrence outcomes.

Counter–cyber operations require defender detection of adversary intrusion and attack activity, and characterization of associated C2 and other supporting infrastructure. Where the defender is unaware of adversary presence or capability, they are unable to affect outcomes of interactions between the intrusion set operators and their intended targets. It is for this reason that contests in the cyber domain are often compared in analogy to antisubmarine warfare problems. Although there are limits to this analogy, it has been extended even to the institutional establishment of major service cyber components, including the U.S. Navy's Tenth Fleet force structure, which takes its lineage from earlier efforts to address detection and response problems posed by adversary offensive capabilities in other domains.[84]

Hider-finder competitions in other strategic domains have since become common, and form a key feature of other strategic interactions in cases involving mobile missile transporter erector launchers and various silo basing force designs including terrain masked and shell game concepts of operation.[85] These characteristics pose known challenges for deterrence interactions, but have to date been considered within the context of diplomatic, intelligence, and counterforce targeting problems. However, novel features arise when these interactions take place within the cyber domain.

Unlike maritime or space domains, adversary deployed capabilities do not maneuver in a commons. Adversary access and supporting infrastructure for strategic effects delivery depends on compromise of systems and networks operated by, or interacting with, their potential targets. These include nodes that exist in "gray space," those areas of cyberspace controlled neither by the adversary nor by defenders. Such gray space is often in practice materially uncontrolled, if not fully ungoverned.[86] Adversary conversion of gray space to their control may occur concurrent to other legitimate uses of these systems

by neutral actors, where the targeted node owners and operators are unaware of compromise. This intermingling of malicious and legitimate activity becomes especially frequent where administrators have not effectively secured their architectures nor made sufficient effort to obtain situational awareness, as is common among systems and networks sought by adversaries for abuse. Unlike in the kinetic domains, adversary access to, and subsequent maneuver in and through, compromised nodes is merely deployment of capability in specific instantiation. Action against these instances is therefore not the same as action against the forces that generate these instances. These critical distinctions mean that existing counterforce paradigms do not fit the contours of operational actions against adversary deployed capabilities (as opposed to the forces that generate, sustain, and employ them). This especially true where actions may occur at the malware layer, involving effects delivered only against implants or implant C2 communications, vice the whole of the system and network nodes where that malware is resident during adversary intrusion.

Counter–cyber operations therefore provide unique opportunities to "unload the gun" held by the adversary in a duel rather than simply to "kill the archer" as in counterforce targeting. Again, as these are not typically single engagement outcomes, it may be better to think of these options as "unloading a brace of guns," where the adversary has multiple dueling pistols arrayed before them.[87] Counter–cyber operations measures may deliver effects across the entirety of an adversary's deployed capabilities, or C2 and other supporting infrastructure, in a course of action intended for takedown objectives. These may be accomplished to varying degrees of partial or full success that fulfill the defender's planned intent, as in any contest of arms, and an adversary may have different options to regenerate these capabilities across different timelines. The defender may also pursue a suppression course of action, either deliberately as an alternative objective to full takedown, or as the accepted result of only partial takedown success, in which an adversary's capabilities are degraded across differing temporal or functional scope. Defenders may also deceive adversary operators as to the extent of their access

and effects options, providing decoy targets or limiting the scope of attacker visibility to exclude higher value targets.

The adversary's "gun" may also be "unloaded silently," without the adversary's awareness, if the CCO action is executed using previously unknown vulnerabilities or where the adversary does not maintain sufficient "state of health" monitoring over deployed capability instances. In these cases, the adversary may only become aware of the erosion of capability when assessing post-strike effects (for example, during battle damage assessment). In some scenarios, even where a defender is unable to change effects delivery outcomes, they may be able to deceptively influence command and control through CCO techniques, and thereby alter perceptions of strike effectiveness. Depending on the nature of adversary intelligence capabilities supporting effects assessment, they may or may not recognize the various root causes of the lack of effects on targets. In services whose officers may have lower integrity or face less individual and organizational accountability, failures resulting from CCO blunted strategic strikes may also be concealed from leadership, or otherwise downplayed when reporting results. This has implications for restrike decisions in partial exchange scenarios. (These are discussed further below.)

"Silent unloading" scenarios also arise where defenders may leverage CCO to conduct extended remediation, subverting adversary's own C2, or flaws in malware designs, to remove implants from targeted systems and networks. These capabilities have been employed in both acknowledged responses to adversary intrusion, as well as cases where defenders are alleged to have sought to conceal either the fact of, or the extent of, eviction involving selected systems and networks from adversaries. The most prominent such recent publicly disclosed case occurred in the Department of Justice's response to widespread exploitation of specific vulnerabilities in on-premises deployments of the Microsoft Exchange email infrastructure, attributed to China nexus HAFNIUM intrusion set and associated operators.[88] Although there are no indications of adversary destructive or disruptive action in these intrusions, the extensive access achieved by the intrusion campaign must be

considered in evaluating future potential offensive effects scenarios and such extended remediation engagements blunt not only the most likely intended espionage value of these accesses, but remove the strategic latency afforded to the adversary by footholds for capabilities to be deployed in later crisis.

Counter–Cyber Operations Concurrent to Defensive Cyber Operations

Counter–cyber operations however are not conducted in a vacuum. Where detection of the adversary arises from defensive cyber operations activities, the complexity of these interactions and their impact on adversary perceptions must be taken into account across the life cycle of the campaign, even where defensive cyber operations are limited to internal defensive measures. Defenders may variably interpret detected adversary active effects operations as "mere" cyber espionage, or as operational preparation of the environment for delivery of attack effects. Each interpretation on detection will suggest different optimal courses of action. In response to espionage, defenders may provide specific warning to support defensive cyber operations that will harden immediate targets against attacker tooling and tradecraft, wider warning for enhanced defensive cyber operations across other potential targets, or engage in defensive cyber operations measures intended to deceive the adversary about the information it has sought to steal from defended systems and networks. Hardening alone is however unlikely to contribute to deterrence, as adversaries well understand from prior operational cycles that internal defensive measures are often incompletely implemented even in cases where they might be tailored to specific threat tradecraft. Time and again this has proved to leave space to contest intrusion outcomes, even against prepared defenders. Many skilled offensive teams will merely regard this as an additional motivation should they become aware of defender efforts.

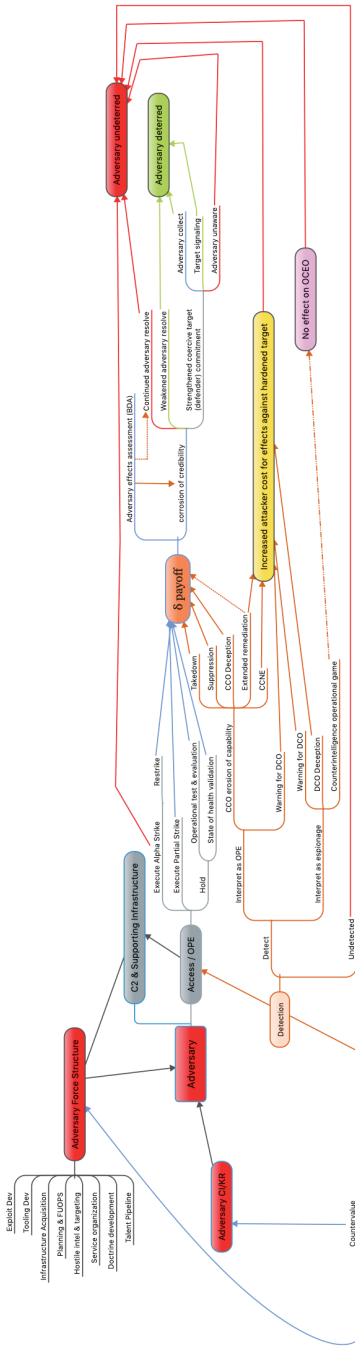
Counter–cyber operations options may also provide defensive contributions beyond warning for hardening. They may provide insight into implants and tooling not yet deployed in targeted networks, burning these before they are observed in the wild. Although the mechanism of discovery has not

been disclosed, some commentators have speculated that this objective of counter–cyber network exploitation may have contributed to early detection of the Pipedream malware in early 2022, before its operational use.[89] Such techniques may also be employed for recurring intelligence collection to provide ongoing visibility into adversary capabilities and intentions, as has been described in multiple private sector efforts targeting weaknesses in criminal botnet infrastructure C2 protocols.[90] Here, the utility of these options is apparent even given the more constrained option set available to operators who must obey domestic computer fraud and abuse laws—legislation that typically would not so limit a state actor.

Each of these defensive courses of action may serve to increase attacker costs to deliver effects against hardened targets. This additional attacker workload has immediate operational impact to scope, scale, and pace of intrusion activities. It also triggers hard resourcing decisions for the adversary in the longer term, where they are forced to evaluate their investment in given capabilities options.[91] In isolation, these factors do not directly impact the calculus of deterrence—merely the considerations of adversary prioritization and continued pursuit of a given operational objective. This is especially so given competing bureaucratic pressures for budget and manpower and the existence of other targets for which capability may be applied toward similar outcomes with less effort. This is consistent with cyber persistence theory explanations that cost imposition is a derived effect of the causal mechanisms used to contest adversary capabilities, including by defending forward.[92]

Some defenders may treat detection of intrusion for espionage intent as a counterintelligence operational game and pursue courses of action intended to characterize adversary requirements (developing "backbearings"), or to create conditions for the further exposure of adversary service tradecraft and associated assets for later action through diplomatic or law enforcement instruments. These approaches, once heavily relied on in early decades of Western attempts to address persistent cyber threats, had generally fallen out of favor as other options became the focus in ongoing intelligence contests.[93] Nonetheless, new advocacy has returned these options to a degree

Figure 3. Deterrence Interactions for Full Range of CCO, DCO, and OCO Counterforce and Countervalue Options



of prominence.[94] Where there is a mismatch between the assessment and actual adversary intent that influences defender course of action selection, the risk of deterrence failure increases. Thus, treating intrusions conducted for operational preparation of the environment as merely a counterintelligence game will likely have no real impact on offensive cyber effects operations deterrence outcomes.

Erosion of Capability and Perceptions of Discounted Payoff

Each of these differing CCO approaches may result in the erosion of capability deployed by the adversary. However, the ultimate impact that this has on the opposition's perception of relative benefits from aggression relative to restraint in the decision to employ offensive cyber effects at strategic thresholds is dependent on relative information about the state of their capability. Counter–cyber operations may cause an adversary to discount potential payoffs from future aggressive actions, but this potential discounted payoff may be recognized only under certain circumstances.

The opposition may detect the impact of countering actions on their deployed capabilities, either because a defender choice deliberately "noisy" execution, or otherwise failed to "silently unload" and was observed by adversary operators. If an adversary recognizes that CCO have eroded their offensive cyber posture, that same adversary may also recognize that this perforce damages the potential deniability of any disruptive or destructive actions leveraging these capabilities. To the extent that their concept of operations, and strategic objectives, rely on such deniability, this may discount the potential payoff for the employment of these options. An adversary may not require full deniability, but merely the prospect of a sufficient separation from full attribution—however implausibly argued—that may serve to blunt flareback and associated political consequences that may arise from military aggression or covert action.[95] However, even in such cases the prospect of facing distinct attribution arising from known compromise of live operational capabilities likely alters these decision equations.

An adversary that is resolved to employ strategic cyber effects in a full and immediate exchange of fires may also not fully understand that their capability has been degraded until after the substantial execution of attempted destructive or disruptive options. Although different adversaries conceptualize such full scope initial fires differently based on their own histories and doctrine, here for simplicity we will refer to this as an "alpha strike" (drawing on naval strike warfare terminology that described allocation of most of the complement of a given platform). In such scenarios, beyond the operational level outcomes of damage limitation resulting where adversary capabilities do not perform to their expectations, CCO may only contribute to deterrence when the adversary considers whether to launch additional restrikes after this alpha strike.

Discussions of deterrence games whose changes to an adversary's decision calculus involving later stages of strategic fires exchanges may be critiqued in that these are triggered only when deterrence has already failed to prevent adversary attack and conflict has been initiated. At the very least, this may be said to shift the discussion to focus on intra-conflict deterrence effect. Nonetheless, as in much of the prior work on nuclear counterforce options, an adversary is not confined to choices between unlimited attack and restraint.[96] Critically, the opposition will of course also know this going into a conflict—and this will affect choices accordingly. Under most exchange scenarios, we may anticipate varying models of limited cyber fires conducted for different targeting, shaping, and escalation objectives. This creates valid deterrence objectives that may alter adversary choices in the sequencing of capabilities (and capabilities held back) in limited strike scenarios.

Where an adversary has instead chosen only to execute an initial partial strike using a limited subset of overall strategic effects delivery capabilities against a given geography or sector, in accordance with varying operational planning options, the adversary may better understand the effects of CCO which have eroded their capabilities. This is likely to more strongly influence uncertainty around the reserved capabilities sets that the adversary chose to hold back. This discounts prospective payoffs from further strike options. It

may also trigger higher order effects within the adversary's own service level behaviors, such as capability stand downs intended to allow for evaluation of failure modes, or to free up resources for new attempts to revive degraded capabilities through surge operations. In cases when such service actions give further reason to doubt the viability of certain capabilities—particularly across those offensive cyber portfolios known to be particularly perishable in the face of disclosure—the opposition's own decisionmaking environment may exacerbate the impact on leadership perceptions. In short, the adversary operators' (and their managers') own worries around this uncertainty may magnify whatever actual erosion of capability was achieved (and may indeed be a higher order influence objective in the design of well-planned CCO concept of operations).

Adversaries may also recognize the erosion of their capability under conditions other than during the conduct of strike operations. Several hostile military and intelligence services choose not to validate prospective effects portfolios under controlled conditions such as in a cyber range (for various reasons related to cost, bureaucratic incentives, and operational limitations), but rather pursuing approaches that replicate operational test and evaluation processes "in the wild" during intrusions against live system and network targets. These are often smaller scale intrusion activities, conducted for narrow demonstrative objectives, or even intended to go unobserved among the wider background noise of constant malicious behavior from the larger number of unattributed, ego motivated, hacktivist, or criminal actors.[97] Likewise, some adversaries may conduct "state of health" monitoring to validate their deployed infrastructure and associated intrusion accesses at various periodicity, providing occasion to recognize the greater uncertainty of effects delivery than may have initially been understood in planning conditions that assumed uncontested, or less challenging, environments. Although the range of opportunities for CCO campaigns to erode capabilities under these conditions are likely rarer, these interactions do potentially provide chances for the adversary to recognize the greater uncertainty in their concepts of operations and/or applied tooling. Earlier understanding of eroded capability may

in some conditions result in adversary's recognition of discounted payoffs, even as in others it may inspire further attempts to solve for such uncertainty through differing engineering methods. Even in the latter case, a concept of operations that fails validation—especially one that fails "in the wild" rather than in a cyber range where operators and planners may argue against what they may see as artificial test conditions—will see uncertainty accrue for some period of time, as teams involved go back to the drawing board.

Counter–cyber operations that erode capabilities also may serve to corrode credibility of the threat posed by that adversary's offensive cyber instrument, both in the minds of the attacker and in the targets of coercion (defenders). Credibility is undermined where the CCO introduces uncertainty into the attacker's ability to carry out its threat, as well as where earlier costly signals intended to strengthen defender perceptions of the potential for damage from the threat are undermined by new facts on the wire. Critically, these are net assessment problems—both attackers' and defenders' perceptions around "correlation of forces" are changing because of these interactions. International relations scholarship has highlighted the central role of such assessments of capability to execute on specific threats as a core dynamic of credibility, as described by Current Calculus theory. This emphasizes the importance of continually revisited perceptions of military capability, over impressions formed by past behavior.[98]

Opposition leadership that understands the loss of their forces' ability to execute on a given strategic effects delivery option may therefore falter in, or even lose, their resolve to continue with an aggressive course of action. In these cases, CCO will have contributed to integrated deterrence outcomes. (It is unlikely that we will be able to say that CCO alone deterred aggression in such instances, as no causal mechanism is likely to operate entirely in isolation in contemporary and future crisis, across the multidimensional and multi-domain span of interactions between states, services, and private actors.)

Defenders facing aggression may further challenge adversary resolve by additional measures which demonstrate their own continued commitment to

resisting threats. The fact of a successful CCO to erode adversary capability is itself such a measure, but the value of this mechanism may be enhanced by additional changes to posture, diplomatic engagements (overtly or in backchannel), or by interactions with private sector entities salient to the adversary's objectives. In order to change adversary perceptions of relative commitment, the opposition must either have adequate intelligence capacity to collect against the observables of these altered defender behaviors, or else they must receive, find intelligible, and correctly interpret other deliberate signals. Where this is not true, and the adversary remains unaware of the CCO campaign and/or associated additional measures, they may persist undeterred.

Counter–cyber operations also undermine an adversary's sunk costs expended in the development of a strategic offensive cyber effects capability. The commitment of resources such as those involved in military preparations for conflict, in this case in and through cyberspace, are considered mechanisms by which an adversary may strengthen coercive threats.[99] Counter–cyber operations serve to reduce the value of these measures as a costly signal to potential coercive targets (defenders), corroding the credibility of threats that may leverage these capabilities (explicitly or otherwise). The relative degree to which the adversary understands this loss of signaling value is dependent on the extent to which they are aware of defender knowledge of a capability prior to its degraded or disrupted state, including how they have sought to signal the existence and fearsome qualities of a capability that generally cannot be disclosed in relevant specific detail without risking potential loss.

Counter–cyber operations that successfully erode adversary capabilities further challenge that adversary's reputation for resolve. Reputation is shaped by past actions that condition expectations of future behavior.[100] Reputation is also strongly predicated on observability—that is, the ability of an audience to see present actions—that will inform expectations of future behavior.[101] This is not assured in the cyber domain for all possible audiences, given the opacity of the environment. But an adversary that has previously demonstrated capabilities to deliver effects in and through the cyber domain against

multiple targets in earlier campaigns that have been disclosed (either publicly, or within specialist communities of practice) builds this reputation through proficiency, relative sophistication, and demonstrated realization of intent to pull the virtual trigger under differing conditions. These reputational benefits accrue even in cases where the operational objectives fall below the threshold of strategic effects, but where the features of a given campaign suggest that a capability may be generalized or adapted beyond specific targets to deliver wider strategic value.

Unlike in the nuclear domain, the constant contact with offensive cyber capabilities whose value derives from use rather than mere possession thus under routine circumstances serves to reinforce this reputation to most knowledgeable observers with sufficient intelligence and situational awareness across relevant target sets. But reputation forms and changes over time in response to repeated interactions, and much of this is grounded in defenders' perception of opposition behavior during negotiations and in crisis, which in some circumstances appears more strongly influenced by assessment of the adversary leader's available military power (although the degree of this influence varies under other contextual circumstances).[102] Here, knowing that a (cyber) military capability is degraded would seem highly likely to change the defender's understanding of the adversary's resolve. And where the adversary's leader is aware of changes to the defender's beliefs, it may indeed sap such resolve.

Yet some adversaries may choose to persist, or even double down, despite the knowledge that their potential payoff for aggression has been discounted by the erosion of their capabilities. These adversaries who demonstrate continued resolve, therefore, represent deterrence failures. These cases do not, however, invalidate the mechanism of deterrence by erosion, but rather are an expected outcome for those opposition leaders that have a higher propensity toward risk taking in pursuit of their objectives, or higher tolerance of the potential downside costs of campaign failure.

This places adversary leaders, and their psychology, at the center of any analysis of potential deterrence outcomes. This centrality poses challenges to

systematic and generalizable assessment, but recent scholarship has shown that these challenges may be overcome by appropriate methodological design and precision.[103] Decisionmaker variables further challenge cyber conflict research, however, in that these are fundamentally political science and political psychology puzzles—not essentially cyber questions (although the unique features of the cyber domain will almost certainly play out distinctively in those puzzles). This is not unexpected in the history of studying wars and the prospect of wars to come, and once again points to the primacy of the human intelligence discipline in resolving unknowns of leadership intent. These questions have become more difficult in the era of renewed Great Power competition (if ever they were at all easier in Cold War or post–Cold War transitional periods).[104]

Structural Imperatives Toward Persistence and Conditionality in Deterrence by Erosion of Capability

These are highly iterated games. The adversary may recognize in specific interactions discounted payoffs from the erosion of offensive cyber capabilities, and the corrosion of the credibility of the threats these capabilities may pose as options to hold targeted systems and networks at risk, contributing to immediate deterrence outcomes. However, these interactions occur in ecosystems under constant change, where new technologies and new functional business processes alter the option space with each generation of Moore's law and its continued downstream reflections.[105] Cyber persistence theory argues there is a structural imperative within the cyber domain that will drive continued attempts to generate power through exploitation of pervasive vulnerability across each of these iterations. Dynamic change creates overarching incentives that limit the circumstances under which an adversary might discount the relative benefits of an aggressive course of action, if not preclude entirely the further influences that defenders may exert on adversary decisionmakers towards deterrent outcomes.

This structural imperative to persist, overriding deterrent outcomes, offers strong explanatory value across a variety of interactions. I concur that

this is likely true for cyber-focused deterrence through punishment (at least for reciprocal in domain actions, or cross-domain retaliation below nuclear thresholds), and given the demonstrated failures of deterrence by denial and norms-centered approaches almost certainly holds true for these mechanisms as well. This may hold true generally across the space of interactions encompassing adversary espionage, and perhaps even many forms of covert action, in the spectrum of competition and subcrisis maneuvering below the threshold of acknowledged armed conflict. Further, removing specific options from the adversary's decision space at a given point in time may be unlikely to preclude the opposition from seeking to re-posture for such options at a future point in time, given the advantages offered by possession and continued utility.

Thus, CCO campaigns which successfully erode an adversary's capabilities as deployed in a given instantiation against specific relative configurations of target objectives may only provide contributions toward integrated deterrence outcomes under some scenarios. This is nonetheless a nonzero number of potential interactions. The timing, and immediacy, of uncertainty introduced into an adversary's plans for strategic offensive cyber effects delivery is likely to be most salient. The prospective futures under which the imperatives to persist and correct for these factors of uncertainty through engineering or operational measure may well exceed the timelines under which decisions toward aggressive courses of action must be made within the context of militarized crisis or ongoing conflict. Under these conditions, discounted payoffs from uncertain cyber capabilities execution may well have greater decision impacts, especially where they undermine linchpin tenants of an adversary's bargaining stance or theory of victory that relies on the capabilities now in question.

It is however precisely these conditions of strategic exchange, at the moments of transition from militarized crisis and into conflict, or in escalation from local conflicts and limited engagement scenarios into wider regional confrontation, where the potential contributions to integrated deterrence may matter most. Pacing and acute threat doctrine has envisioned obtaining early advantage from strategic cyber effects capabilities employment under a variety of war initiation models.[106] Eroding these capabilities, and corroding

credibility of coercive threats, is perhaps more likely here to alter decision calculus around courses of action for aggression than in a general period within the punctuated equilibrium of initial deployment, contested presence, and persistent revisit.

Conclusions

The long-standing disputes over the efficacy, and appropriate pursuit, of strategies of deterrence against cyber threats have faltered for decades. I argue that this is the result of a fundamental mismatch between the kind of contest we have thought we needed to pursue vice the contest that multiple state and nonstate actors have been engaged in throughout the course of real-world operations. This mismatch has led to failures of deterrence, where the adversary has been able to develop and deploy capabilities to hold at risk targets at thresholds of strategic effect.

That such capability has not been generally used is perhaps as much the result of the unusual period in which there has been peace between great powers over the multiple decades of the post–Cold War era, as it is a matter of adversary restraint.[107] The overarching role of the nuclear deterrent umbrella almost certainly also plays a part, to some degree of cross-domain deterrence. Yet, as is well understood in other domains, a ceiling on the highest end of strategic exchange imposed by the stable nuclear deterrence balance creates conditions for more frequent and extended conflict below that threshold: the stability–instability paradox. The implications for this paradox in the cyber domain have previously been taken up by other scholars.[108] This work reinforces the salience of such puzzles when considering the cross-domain dynamics of integrated deterrence.

Nonetheless, within the cyber domain the question of how to effectively deter adversary aggression continues to matter intensely, with salience both for actions conducted only in and through the domain as well as in the engagements that may occur in concert with other instruments of military power projection in crisis and conflict. Counter–cyber operations have demonstrated value at the operational level in setting and resetting the conditions for

security on the network, as described in the language of cyber persistence theory. By removing options for exploitation from the adversary's reach, this concurrently denies the adversary the strategic choice to pursue specific effects against given systems and network targets. This becomes particularly salient where adversary the seeks to employ such offensive effects toward a *fait accompli*.[109] "Resetting" interactions have most recently been observed in campaigns publicly reported to have been conducted against ransomware continuing criminal enterprises in late 2021, and to erode Russian attributed offensive capabilities postured against Ukraine and other European allies in advance of Russia's renewed invasion in February 2022.[110] Connecting these campaigns and their outcomes to the logics of broader national defense strategy has to date remained challenging. Yet it is understandable that such alignment is needed, especially where allies and partners continue to struggle with linking the new paradigms of cyber persistence to broader defense and strategic thinking. Earlier analytic approaches offering a "dual lens" on major campaign cases have provided some explanatory value toward bridging the two theoretical worlds.[111] However, continued demand signal from key decisionmakers indicates that this has as yet remained insufficient.

The concept of pursuing deterrence through the erosion of capabilities offers a new mechanism by which to connect the campaigning necessary to create and sustain conditions for security through cyber capabilities whose value arises out of ongoing interactions, rather than reserved potential. Although these ideas build on earlier insights from well-validated international relations theorists, the extension into the cyber domain requires a fundamental re-orientation that recognizes the potential deterrent value of these dynamics, not merely the escalatory potential that arises in the nuclear domain under conditions where deterrence stability may be threatened.

This is not to say that all CCO will not be escalatory, nor that they may not create such pressures in complex cross-domain interactions. However, one may not presume that escalation pressures accumulate *by default* due to the very different conditions that prevail at the current moment in and through the cyber domain. It remains vitally important to understand the

unique circumstances under which such escalation may be more likely to occur out of the specific features and equities of those conditions encountered live "on the wire."[112] Yet this is not an argument against the conduct of CCO, nor the deliberate pursuit of contributions to integrated deterrence through the cumulative outcomes of CCO campaigns.

It is also important to understand in scoping what kind of contest one will pursue in order to understand where in the spectrum of competition and conflict that such contributions to deterrence will be effective. This analysis is scoped to the question of actions at or beyond the threshold of armed conflict equivalent actions intended to deliver strategic effects. This does not preclude other interactions across lesser dimensions of high intensity crime, ongoing espionage, and covert action for more limited objectives. But it is also vital to understand that adversary offensive cyber capabilities for strategic missions are built on the basis of these campaigns playing out below the threshold. The key accesses, novel exploitation techniques, and new implant designs that matter most to future strategic effects campaigns start on the basis of insights from the constant contact of other forces for other objectives. In cases where longer lead time development options are not possible in a rapidly emerging crisis, or in other "cold start" or "bolt from the blue" scenarios, an adversary may leverage the strategic latency present in pervasive vulnerability to create new assemblages of opportunity and capability to deliver prompt effects.[113] Deterrence postures built on erosion of adversary capabilities must also contend with these dynamics, along with challenges of potential rapid arsenal regeneration offered by "redsourcing" procurement strategies, that effectively outsource tooling development to the commercial penetrating testing industry.[114]

However, this analysis does show why earlier critiques of the ineffectiveness of actions aimed at contributing to deterrence by other mechanisms may indeed be validated. One may note that efforts that merely force additional adversary investment (in time, resourcing, and talent) are unlikely to change overall perceptions of payoff due to the pervasive character of systems and network vulnerability, and the commutability of other attack surfaces toward

the same objectives. In a similar fashion, deterrence by denial via vulnerability reduction is shown to be theoretically misaligned, as much as it may remain as a practical matter out of reach in ecosystems burdened by ever-accumulating legacies of technical debt. Likewise, the mismatch of counterintelligence approaches to deterrence outcomes is clearly illustrated.

Focusing on deterrence by erosion of capabilities does highlight the essential and central role of initiative in these interactions. The advantage that accrues to the actor that recognizes an opportunity for exploitation, and can act with more agility to maximize utility from these options, is distinct in these interactions. This may nonetheless be distinguished from the element of surprise. Although the tradecraft that may be employed to accomplish specific technical actions toward the erosion of adversary capability is more effective within some gradient of secrecy, and in some cases may hinge on it, this does not always imply that an adversary will be (or must be) surprised. They must merely fall behind in the contest of initiative. Some senior scholars have contended that surprise is inevitable.[115] However, we need not accept this as a foregone conclusion where the adversary seeks to deny its realization, nor hold back operations where surprise cannot be assured, for the contributions to deterrence envisioned here do not depend on this condition. These observations on the centrality of initiative are also congruent with explanations offered by cyber persistence theory, further strengthening the connective tissue between strategies under this alternative paradigm with their cumulative contributions to integrated deterrence.

New recognition of the dynamics of deterrence by erosion of capability as the cumulative outcome of CCO campaigning is only the first step in unpacking its contributions to integrated and tailored deterrence strategies. Further research is needed to better understand the microfoundations of capability generation and employment as pillars of credibility and key factors of decisionmaker resolve, especially where perceptions of such capabilities change over time or under crisis pressure (and as their technical features may be incompletely understood by leadership at various levels of remove from the keyboard). Counter–cyber campaigns may be executed under a number

of different concepts of operations, which may have both unique implications for the efficacy of erosion as well as the potential for adversary regeneration or reconstitution within relevant crisis timelines. These contests hinge on initiative, but also comparative intelligence advantage, wherein information asymmetries are key factors in understanding potential outcomes of restraint or deterrence failure. Likewise, the critical role that various signaling options may play in these interactions must be further explored—in both explicit and deliberate manifestation, as well as in tacit sensemaking in the face of incomplete, conflicting, and even deceptive information. Additionally, the formal game theory of these interactions may be further developed, with particular focus on duels involving silently unloading guns, as well as cases in which such attempts are inadvertently or through adversary attention rendered unexpectedly noisy. Such quantitative modeling will, of course, complement additional efforts to understanding how adversaries may discount payoffs when facing erosion of strategic cyber effects capabilities. Lastly, this theory must be tested through rigorous case analysis, examining CCO as they have played out "on the wire," to understand further the explanatory value of these concepts, and to improve estimative fidelity for future interactions in competition and militarized crisis.

In sum, recognizing the unique dynamics of CCO contributing to integrated deterrence through erosion of capability, in cumulative outcomes across persistent campaigning, is merely the first step in a broader research agenda that will be needed going forward. The hardest tests of this theory are occurring daily, in largely silent duels iterating between n-dimensional assemblages of threat actors, defenders, and supporting elements across states and the private sector. The need to understand these interactions becomes only more acute as various global crisis events drive additional actors to seek coercive capabilities in and through the cyber domain, and to find new opportunities to employ these capabilities as substitute strategic options to hold U.S., allied, and partner interests at risk.

Notes

[1] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort George G. Meade, MD: U.S. Cyber Command, April 2018).

[2] Doctrinal definitions of this terminology are at present sadly poor, resulting in often muddled discussion of differing courses of action, with divergence notable between Department of Defense (DOD) writings and those concepts in use elsewhere within the community of practice.

[3] Michael P. Fischerkeller, "What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?" *Lawfare*, May 3, 2022.

[4] Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1991), chapter 1.

[5] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), 381–393.

[6] The author is indebted to Michael Fischerkeller for emphasis on this point, even as he and his coauthors may disagree with my further interpretation.

[7] Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (January 1979); Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy* 31, no. 1 (2010), 1–33; Austin Long, *Deterrence: From Cold War to Long War* (Santa Monica, CA: RAND, 2008).

[8] Bernard Brodie, "Nuclear Weapons: Strategic or Tactical?" *Foreign Affairs*, January 1954; Morton A. Kaplan, "The Calculus of Nuclear Deterrence," *World Politics* 11, no. 1 (October 1958), 20–44; Bernard Brodie, "The Anatomy of Deterrence," *World Politics* 11, no. 2 (January 1959), 173–192; William Kaufmann, "The Requirements of Deterrence," in *Military Policy and National Security*, ed. William Kaufmann (Princeton: Princeton University Press, 1956); Science Advisory Committee, Security Resources Panel, *Deterrence and Survival in the Nuclear Age* (Washington, DC: Office of Defense Mobilization, November 7, 1957, declassified); Thomas W. Milburn, "What Constitutes Effective Deterrence?" *The Journal of Conflict Resolution* 3, no. 2 (June 1959), 138–146; Glenn H. Snyder, *Deterrence by Denial and Punishment* (Princeton: Woodrow Wilson School of Public and International Affairs, Center of International Studies, Princeton University, January 1959); Herman Kahn, *The Nature and Feasibility of War and Deterrence* (Santa Monica, CA: RAND, 1960); Glenn H. Snyder, "Deterrence and Power," *The Journal of Conflict Resolution* 4, no. 2 (June 1960), 163–179; Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960); Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961); Malcolm W. Hoag, "On Stability in Deterrent Races," *World Politics* 13, no. 4 (1961), 505–527; James R. Schlesinger, *Some Notes on Deterrence in Western Europe* (Santa Monica, CA: RAND, 1962); Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966); Klaus Eugen Knorr, *On the Uses*

of Military Power in the Nuclear Age (Princeton: Princeton University Press, 1966); Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Robert H. Kupperman and Harvey A. Smith, "Strategies of Mutual Deterrence," *Science* 176, no. 4030 (1972), 18–23; Warner R. Schilling, "U.S. Strategic Nuclear Concepts in the 1970s: The Search for Sufficiently Equivalent Countervailing Parity," in *New Directions in Strategic Thinking*, ed. Robert O'Neill and D.M. Horner (London: Routledge, 1981); Charles L. Glaser, "Implications of Reduced Vulnerability for Security in the Nuclear Age" (Ph.D. diss., Harvard University, 1983); Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989); Charles L. Glaser, *Analyzing Strategic Nuclear Policy* (Princeton: Princeton University Press, 1990).

[9] Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, and Company, 1977); Nina Tannenwald, "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security* 29, no. 4 (Spring 2005), 5–49; T.V. Paul, *The Tradition of Non-Use of Nuclear Weapons* (Stanford, CA: Stanford University Press, 2009); Posen, *Inadvertent Escalation*; James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018), 56–99; Ali Jafri & John Stevenson, *Space Deterrence: The Vulnerability-Credibility Tradeoff in Space Domain Deterrence Stability* (Arlington, VA: Strategic Multi-Layer Assessment, April 2018); David C. Logan, "Are They Reading Schelling in Beijing? The Dimensions, Drivers, and Risks of Nuclear-Conventional Entanglement in China," *Journal of Strategic Studies* 46, no. 1 (2020).

[10] Lawrence Freedman, *Deterrence* (Cambridge, MA: Polity Press, 2004).

[11] John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1985); Richard J. Harknett, "State Preferences, Systemic Constraints, and the Absolute Weapon," in *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order*, ed. T.V. Paul, Richard J. Harknett, and James J. Wirtz (Ann Arbor: University of Michigan Press, 1996), 52–53; James J. Wirtz, "How Does Nuclear Deterrence Differ from Conventional Deterrence?" *Strategic Studies Quarterly*, Winter 2018, 58–73.

[12] Kaufmann, "The Requirements of Deterrence."

[13] Edward Rhodes, "Nuclear Weapons and Credibility: Deterrence Theory Beyond Rationality," *Review of International Studies* 14, no. 1 (January 1988), 45–62.

[14] Patrick Morgan, "Saving Face for the Sake of Deterrence," in *Psychology and Deterrence*, ed. Robert Jervis, Richard Ned Lebow, and Janice Gross Stein (Baltimore: Johns Hopkins University Press, 1985), 125.

[15] Vesna Danilovic, "The Sources of Threat Credibility in Extended Deterrence," *The Journal of Conflict Resolution* 45, no. 3 (2001), 341–369; Daryl Press, *Calculating Credibility: How Leaders Assess Military Threats* (Ithaca, NY: Cornell University Press, 2005).

[16] Alex Weisiger and Keren Yarhi-Milo, "Revisiting Reputation: How Past Actions Matter in International Politics," *International Organization* 69, no. 2 (2015), 473–495; Keren Yarhi-Milo, *Who Fights for Reputation: The Psychology of Leaders in International Conflict* (Princeton: Princeton University Press, 2018).

[17] Uri Bar-Joseph, "Variations on a Theme: The Conceptualization of Deterrence in Israeli Strategic Thinking," *Security Studies* 7, no. 3 (1998), 145–181; Doron Almog, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4 (Winter 2004), 4–19; Thomas Rid, "Deterrence Beyond the State: The Israeli Experience," *Comparative Security Policy* 33, no. 1 (2012), 124–147.

[18] Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington, DC: NDU Press, 1996); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Adam Segal, "Can U.S. Deter Cyber War?" *The Diplomat*, January 12, 2012; National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010); Panayotis Yannakogeorgos and Adam B. Lowther, "The Prospects for Cyber Deterrence," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis Yannakogeorgos and Adam B. Lowther (London: Taylor & Francis, 2010); Kenneth Geers, "The Challenge of Cyber Attack Deterrence," *Computer Law & Security Review* 26, no. 3 (2010); Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security," *George Washington University*, June 1, 2011; Eric Sterner, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011), 62–80; Richard Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek Reveron (Washington, DC: Georgetown University Press, 2012); Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 77 (2nd Quarter 2015), 8–15; Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017), 44–71; Richard J. Harknett and Joseph S. Nye, Jr., "Is Deterrence Possible in Cyberspace?" *International Security* 42, no. 2 (2017), 196–199; Ben Buchanan, "Cyber Deterrence Isn't MAD; It's Mosaic," *Georgetown Journal of International Affairs*, 2014, 130–140; Aaron F. Brantly, "Entanglement in Cyberspace: Minding the Deterrence Gap," *Democracy and Security* 16, no. 3 (2020), 210–233.

[19] Jon Lindsay and Erik Gartzke, "Cybersecurity and Cross-Domain Deterrence: The Consequence of Complexity," in *U.S. National Cybersecurity: International Politics, Concepts, and Organization*, ed. Damien Van Puyvelde and Aaron F. Brantly (New York:

Routledge, 2017), 11–27; Jacquelyn Schneider, "Cyber and Cross Domain Deterrence: Deterring Within and From Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Eric Gartzke and Jon Lindsay (Oxford: Oxford University Press, 2019).

[20] Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010), 102–135; Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict & Security Law* 17, no. 2 (2012), 229–244; Clement Guitton and Elaine Korzak "The Sophistication Criterion for Attribution," *The RUSI Journal* 158, no. 4 (2013), 62–68; Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015), 53–67; Amir Lupovici, "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward," *International Studies Perspectives* 17, no. 3 (2016), 322–342; Ben Buchanan, *The Legend of Sophistication in Cyber Operations* (Cambridge, MA: Belfer Center for Science and International Affairs, January 2017); Aaron F. Brantly, "The Cyber Deterrence Problem," in *10th International Conference on Cyber Conflict: Maximising Effects*, ed. Tomás Minárik, Raik Jakschis, and Lauri Lindström (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE] Publications, 2018); Sandeep Baliga, Ethan Bueno De Mesquita, and Alexander Wolitzky, "Deterrence with Imperfect Attribution," *American Political Science Review* 114, no. 4 (2020), 1155–1178; David Blagden, "Deterring Cyber Coercion: The Exaggerated Problem of Attribution," *Survival* 62, no. 1 (2020), 131–148; Florian J. Egloff, "Public Attribution of Cyber Intrusions," *Journal of Cybersecurity* 6, no. 1 (2020); Jonathan Welburn, Justin Grana, and Karen Schwindt, "Cyber Deterrence with Imperfect Attribution and Unverifiable Signaling," *European Journal of Operational Research*, 2022.

[21] Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017), 452–481; Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony," *Journal of Strategic Studies* 40, no. 7 (2017), 898–926; Andrew Liaropoulos, "The Uses and Limits of Cyber Coercion," *European Conference on Cyber Warfare and Security*, June 2018.

[22] Edward Geist, "Deterrence Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015), 44–61; Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence In Cyberspace," *Harvard Journal of Law & Technology* 25, no. 2 (2012); Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, MD: Rowman & Littlefield, 2017); Maija Turunen and Martti J. Kari, "Cyber Deterrence and Russia's Active Cyber Defense," *European Conference on Information Warfare and Security*, June 2020; Greg Austin, ed., *National Cyber Emergencies: The Return to Civil Defence* (London: Routledge, 2020); Martin Libicki, "Can Denial Deter in Cyberspace?" in *Deterrence by Denial: Theory and Practice*, ed. Alex

S. Wilner and Andreas Wenger (Amherst, MA: Cambria Press, 2021); Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies*, August 2021, 1–36.

[23] Andrea Locatelli, "The Offense/Defense Balance in Cyberspace," *Italian Institute for International Political Studies*, October 31, 2013; Patrick J. Malone, "Offense-Defense Balance in Cyberspace: A Proposed Model" (master's thesis, Naval Postgraduate School, 2012); Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (2013), 40–63; Keir Lieber, "The Offense-Defense Balance and Cyber Warfare," in *Cyber Analogies*, ed. Emily Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School, 2014), 96–107; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015), 316–348; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2016), 72–109; Wade L. Huntley, "Strategic Implications of Offense and Defense in Cyberwar," in *49th Hawaii International Conference on System Sciences* (New York: Institute of Electrical and Electronics Engineers [IEEE], 2016); Jason Healey, "The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities," in *Bytes, Bombs, Spies: The Strategic Dimensions of Offensive Cyberspace Operations*, ed. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2019), 173–194; Daniel Gipper, "The Cyber Offense-Defense Balance Revisited: The Variables Tipping the Balance" (master's thesis, Naval Postgraduate School, 2020); Charles Smythe, "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance," *Yale Journal of International Affairs*, 2020; Eviatar Matania and Eldad Tal-Shir, "Continuous Terrain Remodelling: Gaining the Upper Hand in Cyber Defence," *Journal of Cyber Policy* 5, no. 2 (2020), 285–301; Jason Healey, "Understanding the Offense's Systemwide Advantage in Cyberspace," *Lawfare*, December 22, 2021.

[24] Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies* 40, no. 1–2 (2017), 92–117.

[25] Alex S. Wilner, "U.S. Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43, no. 2 (2020), 245–280.

[26] Cyber Conflict Studies Association, "State-of-the-Field Conference," Columbia University, June 16–17, 2016, remarks under Chatham House rule.

[27] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2014), 54–67; Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly* 75 (4th Quarter 2014), 43–52; Robert "Jake" Bebber, "There Is No Such Thing as Cyber Deterrence. Please Stop," *The Cipher Brief*, April 1, 2018; Matthias Schulze, "Cyber Deterrence Is Overrated: Analysis of the Deterrent Potential of the New U.S. Cyber Doctrine and Lessons for Germany's 'Active Cyber Defence,'" *Stiftung Wissenschaft und Politik*, 2019; Tuan N. Pham, "In Cyberspace, No

One Can Hear You Bluff," *Center for International Maritime Security*, May 11, 2022; Thomas Johansmeyer, "Cyber Insecurity: Give Deterrence a Break," *Small Wars Journal*, July 2, 2022.

[28] David Agranovich and Mike Dvilyanksi, "Disrupting Cyber Adversaries: Meta's Approach to Deterrence," video, 9:12, CYBERWARCON 2021, Arlington, VA, November 16, 2021.

[29] Lester Godefrey, "An Allied Perspective on Cyber: Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests," *Studies in Intelligence* 66, no. 1 (2022).

[30] Richard Andres, "Cyber Gray Space Deterrence," *PRISM* 7, no. 2 (2017), 90–99; Jason Healey and Neil Jenkins, "Are U.S. Cyber Deterrence Operations Suppressing or Inciting Attacks?" CYBERWARCON, Arlington, VA, November 28, 2018; Alex Wilner, "Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation," *Comparative Strategy* 36, no. 4 (2017); Martin C. Libicki, "Expectations of Cyber Deterrence," *Strategic Studies Quarterly* 12, no. 4 (2018), 44–57; Jason Healey and Neil Jenkins, "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence Is Working or Failing," in *11th International Conference on Cyber Conflict: Silent Battle* (Tallinn: NATO CCDCOE Publications, 2019).

[31] Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (Sebastopol, CA: O'Reilly, 1999); Dan Geer, "Cybersecurity as Realpolitik," Black Hat USA, Las Vegas, August 2–7, 2014; Dan Geer, "For Good Measure: The Undiscovered," *Login* 40, no. 2 (April 2015), 50–52.

[32] Multiple recent real world operational examples may illustrate the point. The simplest are perhaps provided by recurring exploitation focus on common targets such as Microsoft Exchange, producing high impact bugs leveraged in the wild across multiple adversary campaigns over multiple years between December 2020 to September 2022, including CVE-021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-42321, CVE-2022-41040, and CVE-2022-41082.

[33] David Weinberger, *Small Pieces Loosely Joined: A Unified Theory of the Web* (New York: Basic Books, 2002).

[34] Thomas Dullien, "Security, Moore's Law, and the Anomaly of Cheap Complexity," in *10th International Conference on Cyber Conflict* (Tallinn: NATO CCDCOE Publications, 2018).

[35] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022).

[36] Jim Chen, "Deterrence and Its Implementation in Cyber Warfare," 12th International Conference on Cyber Warfare and Security, Dayton, OH, March 2–3, 2017; Jim Chen, "Take the Rein of Cyber Deterrence," in *2017 International Conference on Cyber*

Conflict (CyCon U.S.), Washington, DC, November 7–8, 2017 (New York: IEEE, 2017); Jim Chen, "Cyber Deterrence by Engagement and Surprise," PRISM 7, no. 2 (2017), 100–107; Jim Chen, "On Levels of Deterrence in the Cyber Domain," *Journal of Information Warfare* 17, no. 2 (2018), 32–41.

[37] Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem," *Intelligence and National Security* 36, no. 2 (2021), 260–278; Robert Chesney and Max Smeets, *Deter, Disrupt, Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Washington, DC: Georgetown University Press, 2023).

[38] Lennart Maschmeyer, "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict," *Journal of Strategic Studies*, 2022, 1–25.

[39] *Report* (Washington, DC: U.S. Cyberspace Solarium Commission, March 2020).

[40] Michael Gallagher, "Intelligence and National Security Strategy: Reexamining Project Solarium," *Intelligence and National Security* 30, no. 4 (2015), 461–485.

[41] Joshua Rovner, "Did the Cyberspace Solarium Commission Live Up to Its Name?" *War on the Rocks*, March 19, 2020.

[42] Stefan Soesanto and Max Smeets, "Cyber Deterrence: The Past, Present, and Future," in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans Osinga and Tim Sweijs (The Hague: T.C.M. Asser Press, 2021); Erica Lonergan and Mark Montgomery, "What Is the Future of Cyber Deterrence?" *SAIS Review of International Affairs* 41, no. 2 (2021), 61–73.

[43] "Defining the Research Agenda Conference," Cyber Conflict Studies Association, July 6, 2020, remarks under Chatham House rule.

[44] Barry Schneider and Patrick Ellis, eds., Tailored Deterrence: Influencing States and Groups of Concern (Maxwell Air Force Base, AL: U.S. Air Force Counterproliferation Center, May 2011); Michael Johnson and Terrence Kelly, "Tailored Deterrence: Strategic Context to Guide Joint Force 2020," *Joint Force Quarterly* 74 (3rd Quarter 2014), 22–29; Nuclear Posture Review Report (Washington, DC: DOD, February 2018); "Fact Sheet 2022 National Defense Strategy," DOD, March 28, 2022.

[45] Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017).

[46] John Brunner, *The Shockwave Rider* (New York: Harper & Row, 1975); William Gibson, *Neuromancer* (New York: Ace, 1984).

[47] Craig J. Weiner, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (Ph.D. diss., George Mason University, 2016).

[48] Andrew Futter, "War Games Redux? Cyberthreats, U.S.–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control," *European Security* 25, no. 2 (2016), 163–180; Paul Bracken, "The Cyber Threat to Nuclear Stability," *Orbis* 60, no. 2 (2016), 188–203; Sico van der Meer, "Cyber Warfare and Nuclear Weapons: Game-Changing Consequences?" *Clingendael Magazine*, December 12, 2016; Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (2017), 37–48; Stephen J. Cimbala, "Nuclear Deterrence and Cyber Warfare: Coexistence or Competition?" *Defense & Security Analysis* 33, no. 3 (2017), 193–208; Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, DC: Georgetown University Press, 2018); Jesse T. Wasson and Christopher E. Bluesteen, "Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems," *Defence Studies* 18, no. 4 (2018), 433–453; Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences," *Chatham House*, January 11, 2018; Jon Lindsay, *Cyber Operations and Nuclear Weapons*, Tech4GS Special Reports (Berkeley, CA: Nautilus Institute for Security and Sustainability, June 20, 2019); Michael Klare, "Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation," *Arms Control Today* 49, no. 9 (2019), 6–13; Herb Lin, *Cyber Threats and Nuclear Weapons* (Stanford, CA: Stanford University Press, 2021); Ariel Levite et al., China-U.S. Cyber-Nuclear C3 Stability (Washington, DC: Carnegie Endowment for International Peace, April 2021); Stephen J. Cimbala, "Nuclear-Crisis Management and Cyber War—A Dangerous Crossroads," *Naval War College Review* 75, no. 1 (2022), 5.

[49] Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (2019); Braden C. Soper, "A Cyber-Nuclear Deterrence Game," in *57th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 24–27, 2019 (New York: IEEE, 2019); Benjamin Schechter, Jacquelyn Schneider, and Rachael Shaffer, "Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming," *Simulation & Gaming* 52, no. 4 (2021), 513–526.

[50] Charles L. Glaser and Steve Fetter, "Should the United States Reject MAD? Damage Limitation and U.S. Nuclear Strategy Toward China," *International Security* 41, no. 1 (Summer 2016), 49–98; Brendan Rittenhouse Green et al., "The Limits of Damage Limitation," *International Security* 42, no. 1 (2017), 193–207.

[51] Erik Gartzke and Jon Lindsay, "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence," in Lin and Zegart, eds., *Bytes, Bombs, Spies*.

[52] Austin Long, "Deterrence: The State of the Field," *New York University Journal of International Law and Politics* 47, no. 357 (2015), 357–377.

[53] Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44,

no. 3 (2020), 48–83; David M. Allison et al., "Clandestine Capabilities and Technological Diffusion Risks," *International Security* 45, no. 2 (2020), 194–198.

[54] Martin Libicki, *Brandishing Cyberattack Capabilities* (Santa Monica, CA: RAND, 2013).

[55] Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academies of Sciences of the United States of America* 11, no. 4 (2014), 1298–1303; Max Smeets and J.D. Work, "Operational Decision-Making for Cyber Operations: In Search of a Model," *Cyber Defense Review* 5, no. 1 (2020), 95–112.

[56] J.D. Work, "China Flaunts Its Offensive Cyber Power," *War on the Rocks*, October 22, 2021.

[57] Benjamin B. Fischer, "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps," *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (2014), 431–464.

[58] Weidi Xu, remarks at International Conference on Cyber Engagement, George Washington University, April 23, 2019.

[59] 徐龙第 [Xu Longdi], "网络攻击、核安全和战略稳定m" [Cyber attacks, nuclear security, and strategic stability], 信息安全与通信保密 [Information security and communication secrecy], 2018, 13–19.

[60] Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1–2 (2018), 6–32; J.D. Work, "Calculating the Fast Equations: Arsenal Management Considerations in Sustained Offensive Cyber Operations," seminar, Belfer Center for Science & International Affairs, April 8, 2019.

[61] Michael Fischerkeller, "What Do We Know About Cyber Operations During Militarized Crises?" *Atlantic Council*, January 31, 2022.

[62] Posen, *Inadvertent Escalation*.

[63] Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca, NY: Cornell University Press, 1984); Robert Powell, "Nuclear Brinkmanship with Two-Sided Incomplete Information," *American Political Science Review* 82 (1988), 155–178; Robert Powell, "Nuclear Deterrence and the Strategy of Limited Retaliation," *American Political Science Review* 83 (1989), 503–519.

[64] Caitlin Talmadge, "Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today," *Journal of Strategic Studies* 42, no. 6 (2019), 864–887.

[65] James Wirtz, "Counter Proliferation, Conventional Counterforce and Nuclear War," *Journal of Strategic Studies* 23, no. 1 (2000), 5–24; Tong Zhao, "Conventional Counterforce Strike: An Option for Damage Limitation in Conflicts with Nuclear-Armed Adversaries?" *Science & Global Security* 19, no. 3 (2011), 195–222; Dean Wilkening, "Hypersonic Weapons and Strategic Stability," *Survival* 61, no. 5 (2019), 129–148; Ian Bowers and Henrik Stalhane Hiim, "Conventional Counterforce Dilemmas: South Ko-

rea's Deterrence Strategy and Stability on the Korean Peninsula," *International Security* 45, no. 3 (2020), 7–39; Ian Bowers, "Counterforce Dilemmas and the Risk of Nuclear War in East Asia," *Journal for Peace and Nuclear Disarmament* 5, no. 1 (2022), 6–23.

[66] Gartzke and Lindsay, "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence," in Lin and Zegart, eds., *Bytes, Bombs, Spies*.

[67] J.D. Work, "Intercept Calls: Left of Launch Offensive Cyber Engagement Decisions Involving Limited Ballistic Missile Fires," International Studies Association Annual Convention, March 15–19, 2023.

[68] National Nuclear Security Administration, *Stockpile Stewardship and Management Plan* (Washington, DC: Department of Energy, March 16, 2022).

[69] Edward Moses, "The National Ignition Facility and the National Ignition Campaign," *IEEE Transactions on Plasma Science* 38, no. 4 (2010), 684–689.

[70] Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (2018), 90–113; Max Smeets, "Countering Adversarial Cyber Campaigns," video, 18:22, USENIX Enigma Conference, Burlingame, CA, January 28–30, 2019; Matthias Schulze, "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations," in *12th International Conference on Cyber Conflict*, ed. T. Jancarkova, Lauri Lindström, and G. Visky (Tallinn: NATO CCD-COE Publications, 2020); Tobias Liebetrau, "Cyber Conflict Short of War: A European Strategic Vacuum," *European Security* 31, no. 4 (2022), 1–20; Fiona S. Cunningham, "Strategic Substitution: China's Search for Coercive Leverage in the Information Age," *International Security* 47, no. 1 (2022), 46–92.

[71] Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Jan Kallberg, "Strategic Cyberwar Theory—A Foundation for Designing Decisive Strategic Cyber Operations," *Cyber Defense Review* 1, no. 1 (2016), 113–128; Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," *Journal of Cybersecurity* 3, no. 1 (2017), 19–28; Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (New York: Oxford University Press, 2022).

[72] *National Defense Strategy of the United States of America* (Washington, DC: DOD, 2022), 8.

[73] James McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly* 10, no. 4 (2016), 46–63; Christopher Argles, "A Conceptual Review of Cyber-Operations for the Royal Navy," *The Cyber Defense Review* 3, no. 3 (2018), 43–56; Dennis Granåsen and Margarita Jaitner, "The Offensive Cyber Operations Playbook," *18th European Conference on Cyber Warfare and Security*, 2019; Sung-Joong Kim et al., "A Study on the Operation Concept of Cyber Warfare Execution Procedures," *Journal of Internet Computing and Services* 21, no. 2 (2020), 73–80.

[74] Richard Harknett and Emily Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2 (2016), 81–88.

[75] Gary Brown, "Spying and Fighting in Cyberspace: What Is Which," *Journal of National Security Law & Policy* 8 (2015), 621; Aaron Brantly, "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace," *Intelligence and National Security* 31, no. 5 (2016), 674–685; Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis," *Texas National Security Review* 3, no. 4 (2020), 54–81.

[76] Including proposed space sector and elections infrastructure to the 16 canonical critical infrastructure and key resources designations under original U.S. policy in Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: Cybersecurity & Infrastructure Security Agency, December 17, 2003); "Designating the U.S. Space Sector as Critical Infrastructure," *Intelligence and National Security Alliance*, November 2021; Maria Barsallo Lynch et al., *Beyond 2020: Policy Recommendations for the Future of Election Security* (Cambridge, MA: Belfer Center for Science and International Affairs, February 2021).

[77] Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* 45, no. 4 (2022), 534–567.

[78] Brett Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (2nd Quarter 2014), 12–19.

[79] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019; Julian Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *New York Times*, February 26, 2019.

[80] J.D. Work, "Poll Position: Successful Counter-Cyber Operations Secure U.S. Election," *Jane's Intelligence Review*, January 28, 2021.

[81] "Strategic Intelligence Group Intelligence Guidance: Week of 15 October 2012," Symantec, October 18, 2012.

[82] "Observed Tampering with 'Brobot' DDOS Botnet Supports Assessment That 'Operation Ababil' Paused Due to Outside Intervention," iSIGHT Partners, January 22, 2013; "Brobot DDOS Attacks Against U.S. Financial Sector on Aug. 14, 2013, Employ Altered Infection Code, Probably to Improve Botnet's Resilience," iSIGHT Partners, August 14, 2013; J.D. Work, "Echoes of Ababil: Re-examining Formative History of Cyber Conflict and Its Implications for Future Engagements," Soldiers and Civilians in the Cauldron of War, 86th Annual Meeting of the Society for Military History, Columbus, Ohio, May 9–12, 2019.

[83] J.D. Work, "Offensive Cyber Confidence, Competition and Escalation in Recent Gulf Crisis Events," Workshop on Crisis Stability and Cyber Conflict, Columbia Univer-

sity and Department of Defense Minerva Research Initiative, New York, February 25, 2020.

[84] "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," Fleet Cyber Command/U.S. Tenth Fleet Public Affairs, January 29, 2010.

[85] Stephen Meyer, "Verification and the ICBM Shell-Game," *International Security* 4, no. 2 (1979), 40–68; R. James Woolsey, "U.S. Strategic Force Decisions for the 1990s," *Washington Quarterly* 12, no. 1 (1989), 67–83; John Harvey et al., *Carry Hard ICBM Basing: A Technical Assessment* (Livermore, CA: Lawrence Livermore National Laboratory, 1989); Jeffrey Lewis, "Sino-American Security Relations: The Nuclear Dynamics," in *Asia-Pacific Regional Security Assessment 2022*, (London: International Institute for Strategic Studies, 2022), 110–133; Antonio Calcara et al., "Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare," *International Security* 46, no. 4 (2022), 130–171.

[86] Canonical definition in U.S. doctrine may be found in Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018).

[87] Duelist analogies are of course owed to the generations of game theory scholars, especially David Blackwell, Melvin Dresher, Lloyd Shapely, and other RAND mathematicians and analysts who were so pivotal in describing these interactions in strategic contexts.

[88] "Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities," Department of Justice, April 13, 2021.

[89] "PIPEDREAM at the Disco: Implications for International Security and Operational Technology," video, 1:00:12, Atlantic Council Cyber Statecraft Initiative, April 22, 2022, remarks under Chatham House rule.

[90] Jose Nazario, "Botnet Tracking: Tools, Techniques, and Lessons Learned," Black Hat, Las Vegas, July 28–August 2, 2007; Moheeb Abu Rajab et al., "My Botnet Is Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging," in *Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets*, Cambridge, MA, April 10, 2007 (Berkeley, CA: USENIX Association, 2007); Ben Stock et al., "Walowdac: Analysis of a Peer-to-Peer Botnet," in *2009 European Conference on Computer Network Defense*, Milan, Italy (New York: IEEE, November 2009); Juan Caballero et al., "Dispatcher: Enabling Active Botnet Infiltration Using Automatic Protocol Reverse-Engineering," Conference on Computer and Communications Strategy, in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, November 9, 2009, 621–634; Felix Leder, Tillmann Werner, and Peter Martini, "Proactive Botnet Countermeasures: An Offensive Approach," in *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press, 2009), 211–225; Brett Stone-Gross et al., "Your Botnet Is My Botnet: Analysis of a Botnet Takeover," Conference on Computer and Communications Strategy, in *Proceedings of the 16th ACM Conference on*

Computer and Communications Security (New York: Association for Computing Machinery, November 2009), 635–647; Chia Yuan Cho et al., "Inference and Analysis of Formal Models of Botnet Command and Control Protocols," Conference on Computer and Communications Strategy, in *Proceedings of the 17th ACM Conference on Computer and Communications Security* (New York: Association for Computing Machinery, October 2010), 426–439; David Dittrich, "So You Want to Take Over a Botnet. . . ," in *Proceedings of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats*, San Jose, April 25–27, 2012 (Berkeley, CA: USENIX Association, 2012); Marc Eisenbarth and Jason Jones, "BladeRunner: Adventures in Tracking Botnets," in Botnet Fighting Conference, Nantes, France, December 5–6, 2013; Shankar Karuppayah et al., "On Advanced Monitoring in Resilient and Unstructured P2P Botnets," in 2014 IEEE International Conference on Communications, Sydney, Australia (New York: IEEE, 2014); Bou-Elias Harb, Mourad Debbabi, and Chadi Assi, "Big Data Behavioral Analytics Meet Graph Theory: On Effective Botnet Takedowns," *IEEE Network* 31, no. 1 (2016), 18–26; Leon Böck et al., "Next Generation P2P Botnets: Monitoring Under Adverse Conditions," in *International Symposium on Research in Attacks, Intrusions, and Defenses* (Cham: Springer, September 2018), 511–531; Leon Böck et al., "Autonomously Detecting Sensors in Fully Distributed Botnets," *Computers and Security* 83 (2019), 1–13; Jonathan Fuller et al., "C3PO: Large-Scale Study of Covert Monitoring of C&C Servers via Over-Permissioned Protocol Infiltration," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (New York: Association for Computing Machinery, 2021), 3352–3365.

[91] John Mallory (MIT) and Andrew Thompson (Mandiant) are both proponents of such cost imposition and have commented extensively on attacker workload in multiple forums for years.

[92] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect," *Lawfare*, February 6, 2020.

[93] J.D. Work, "Private Actors and the Intelligence Contest in Cyber Conflict," in *Deter, Disrupt, Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed. Robert Chesney and Max Smeets (Washington, DC: Georgetown University Press, 2023).

[94] Petrus Duvenage, and Sebastiaan von Solms, "The Case for Cyber Counterintelligence," in *2013 International Conference on Adaptive Science and Technology*, Pretoria, South Africa (New York: IEEE, November 2013); Johan Sigholm and Martin Bang, "Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats," in *2013 European Intelligence and Security Informatics Conference*; Petrus Duvenage, Sebastian von Solms, and Manuel Corregedor, "The Cyber Counterintelligence Process: A Conceptual Overview and Theoretical Proposition," in *Proceedings of the 14th European Conference on Cyberwarfare and Security*, Hatfield, UK (Manchester: Academic Conferences and Publishing International Limited, July

2015); Victor Jaquire and Sebastiaan von Solms, "Towards a Cyber Counterintelligence Maturity Model," in *Proceedings of the 12th International Conference on Cyber Warfare and Security*, Dayton, OH (Manchester: Academic Conferences and Publishing International Limited, March 2017); Neil Ashdown, "How Commercial Cyber Threat Intelligence Practitioners Talk About Intelligence and Counterintelligence," Royal Holloway, University of London, August 2020; Thenjiwe Sithole and Jaco Du Toit, "A Cyber Counterintelligence Competence Framework," in *Proceedings of the 21st European Conference on Cyber Warfare and Security*, Chester, UK (Manchester: Academic Conferences and Publishing International Limited, June 2022); Thomas Rid, "On Digital Counterintelligence," Cryptologic History Symposium, U.S. National Security Agency, May 11, 2022.

[95] Rory Cormac and Richard J. Aldrich, "Grey Is the New Black: Covert Action and Implausible Deniability," *International Affairs* 94, no. 3 (2018), 477–494; Michael Poznansky, "Revisiting Plausible Deniability," *Journal of Strategic Studies* 45, no. 4 (2022), 511–533.

[96] R. Harrison Wagner, "Nuclear Deterrence, Counterforce Strategies, and the Incentive to Strike First," *The American Political Science Review* 85, no. 3 (1991), 727–749.

[97] J.D. Work, "Who Hath Measured the (Proving) Ground: Variation in Offensive Capabilities Test and Evaluation," *Proceedings of the 15th International Conference on Cyber Warfare and Security*, Old Dominion University, Norfolk, VA (Manchester: Academic Conferences and Publishing International Limited, March 2020).

[98] Press, *Calculating Credibility*, 20–28.

[99] James Fearon, "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs," *Journal of Conflict Resolution* 41, no. 1 (1997), 68–90.

[100] Schelling, *Arms and Influence.*

[101] Yarhi-Milo, *Who Fights for Reputation*, 6.

[102] Danielle Lupton, *Reputation for Resolve: How Leaders Signal Determination in International Politics* (Ithaca, NY: Cornell University Press, 2020), 58–61.

[103] Yarhi-Milo, *Who Fights for Reputation*, 270–271.

[104] Raymond Garthoff, "On Estimating and Imputing Intentions," *International Security* 2 (Winter 1978), 22–32; Robert Mandel, "On Estimating Post-Cold War Enemy Intentions," *Intelligence and National Security* 24, no. 2 (2009), 194–215.

[105] Gordon Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (1965), 114; Ethan Mollick, "Establishing Moore's Law," *IEEE Annals of the History of Computing* 28, no. 3 (2006), 62–75.

[106] 蒋盘林, "从传统电子战走向信息战：电子战发展简史及信息战的定义与内涵" [From traditional electronic warfare to information warfare: A brief history of electronic warfare and the definition and connotation of information warfare], 电子对抗技术 [Electronic Countermeasures] 20, no. 4 (2005), 3–40; 刁华伟，张建科，"防空信息 系统面临的赛博战威胁 与对 策研究" [Research on cyber warfare threats

and countermeasures faced by air defense information systems], 航天电子对抗 [Aerospace Electronic Countermeasures] 27, no. 5 (2011), 16–18; David Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* 56, no. 4 (2014), 7–22; К.А. Троценко, "Информационное противоборство в оперативнотактическом звене управления" [Information confrontation in the operational–tactical level of command and control], Военная мысль [Military Thought] 8 (2016), 20–25; Simone Dossi, "On the Asymmetric Advantages of Cyberwarfare: Western Literature and the Chinese Journal Guofang Keji," *Journal of Strategic Studies* 43, no. 2 (2020), 281–308.

[107] Jason Healey has made this point persuasively on multiple occasions.

[108] Jon Lindsay and Erik Gartzke, "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in International Politics*, ed. Kelly Greenhill and Peter Krause (New York: Oxford University Press, 2018).

[109] Michael Fischerkeller, "The Fait Accompli and Persistent Engagement in Cyberspace," *War on the Rocks*, June 24, 2020.

[110] Ellen Nakishima and Dalton Bennett, "A Ransomware Gang Shut Down After Cybercom Hijacked Its Site and It Discovered It Had Been Hacked," *Washington Post*, November 3, 2021; Joseph Menn and Christopher Bing, "Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline," *Reuters*, October 21, 2021; Gordon Corera, "Inside a U.S. Military Cyber Team's Defence of Ukraine," BBC, October 30, 2022.

[111] J.D. Work and Richard J. Harknett, "Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges," *Atlantic Council*, July 22, 2022.

[112] J.D. Work, "Burned and Blinded: Escalation Risks of Intelligence Loss from Countercyber Operations in Crisis," *International Journal of Intelligence and CounterIntelligence* 35, no. 4 (2022), 806–833.

[113] J.D. Work, "Rapid Capabilities Generation and Prompt Effects in Offensive Cyber Operations," International Studies Association Annual Convention, Las Vegas, April 6–9, 2021.

[114] Chris Glyer and Nick Carr, "RedSourcing: Cyberwar on a Budget," video, 10:15, CYBERWARCON 2019, Arlington VA, November 21, 2019.

[115] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (1978), 61–89; James Wirtz, "Theory of Surprise," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, ed. Richard K. Betts and Thomas G. Mahnken (London: Routledge, 2004), 110–124.

Contributors

Joseph L. Billingsley is director of Strategic Engagement in the College of Information and Cyberspace (CIC) at the National Defense University (NDU). He focuses on forging and sustaining relationships with a diverse array of critical stakeholders to support the organization's educational mission. He is also the creator of the National Service Panel at the world's largest hacker conference (DEF CON), founder of the nonprofit Military Cyber Professionals Association, an adjunct professor and cyber intelligence advisor at the Institute of World Politics, special advisor of the peer-reviewed journal *Military Cyber Affairs*, peer reviewer for *Joint Force Quarterly*, and creator of the Cyber Embassy Night event series in Washington, DC. He has been adjunct faculty at The George Washington University, advisor of the Cyber Security Forum Initiative, reviewer for the Institute of Electrical and Electronics Engineers, judge at the Atlantic Council's Cyber 9/12 Strategy Competition, and fellow at the Center for Network Innovation and Experimentation.

He is a former U.S. Army strategist (Functional Area 59), cyber warfare officer (17A), and signal corps officer (25A), and was also trained as a military intelligence and signals intelligence officer. In uniform, he served in various executive and staff positions at each echelon from platoon to general staff. His expeditionary activities include a 15-month Surge deployment to

Iraq as part of the 1st Armored Division (Multi-National Division–North), engagement activities in the former Warsaw Pact, being under way on the Mediterranean Sea aboard the USS *Mount Whitney* during the Arab Spring, and earning the highest level of the Military Proficiency Badge from the Bundeswehr.

He is a graduate of programs at the Naval War College, Army War College, Military Intelligence School, and Army School of Information Technology. He holds a BA in History from the University of Connecticut, where he founded the History Club. Selected as the inaugural Army Cyber Scholar, he was first Army student awarded a MS in Cyber Systems and Operations from the Naval Postgraduate School (NPS), where he also earned a graduate certificate in cyber wargaming. He received doctoral training in information sciences at NPS and in cyber leadership at Capitol Technology University.

Rear Admiral Heidi K. Berg, USN, is director, Plans and Policy, J5, at U.S. Cyber Command. She is a 1991 graduate of the U.S. Naval Academy. She studied Russian at the Defense Language Institute in 1992 and Arabic at the Kalimat Institute in Cairo in 2004. Admiral Berg received a Master of Philosophy in modern middle eastern studies and Arabic from St. Antony's College, Oxford University, United Kingdom, in 2005.

Her operational tours include Navy Security Group Activity in Rota, Spain, where Admiral Berg flew over 1,000 hours as a communications intercept evaluator onboard EP-3E aircraft in support of Operations *Provide Promise/Sharp-Guard*. She served onboard the USS *Kidd*, Cruiser Destroyer Group 12 onboard the USS *Saratoga*, and the USS *Key West* while assigned to NSGA Rota. She participated in Fleet Staff talks with the post-Soviet Russian navy in the Mediterranean while at Sixth Fleet aboard the USS *LaSalle* in Gaeta, Italy, followed by a tour at RAF Menwith Hill Station, Harrogate, United Kingdom. In 2012, Admiral Berg deployed to Afghanistan as director of the International Security Assistance Force Red Team at ISAF Headquarters in Kabul. As director, she led alternative analysis and provided strategic assessments recommendations to the ISAF Commander. Following

deployment, Admiral Berg served as deputy for Plans and Policy at Fleet Cyber Command/U.S. Tenth Fleet.

Admiral Berg's command tours include the Navy Information Operations Command in Bahrain (2008–2009) where she was responsible for providing theater airborne and surface signal intelligence support to Operations *Iraqi Freedom*, *Enduring Freedom*, and Persian Gulf maritime operations. She was also the Navy Element Commander of the Defense Intelligence Agency and director of the Joint Military Intelligence Training Center (2013–2015). Her most recent assignment was director of intelligence at U.S. Africa Command.

Staff assignments include airborne signals intelligence requirements officer and information operations strategy and policy on the Chief of Naval Operations staff; deputy national intelligence officer for military issues at the National Intelligence Council; military advisor to the deputy director of National Intelligence, where she supported daily intelligence briefings to the President and provided direct intelligence support to the National Security Advisor, National Security Council, and Congress; information warfare and foreign area officer division director (PERS-47) at Navy Personnel Command, strategic advisor (OOZ) to the Chief of Naval Operations; and acting director of the Navy Digital Warfare Office.

Admiral Berg has been awarded various personal, campaign, unit, and service awards.

Dr. Jim Q. Chen is associate dean and professor in CIC at NDU. He is also the inaugural director of the Department of Defense University Consortium for Cybersecurity (DOD UC2) Coordination Center. In this role, he leads the Coordination Center, which is the administrative chair of the DOD UC2 in helping to achieve the mission to fulfill the intent of the law provide a connection between the Secretary of Defense and the academic community on matters of cybersecurity via requests for information.

Dr. Chen's expertise lies in cyber strategy, cyber deterrence, cyber warfare, cybersecurity technology, artificial intelligence, machine learning, natural language processing, and educational theories. Based on his research, he

has authored and published more than 80 peer-reviewed papers, articles, and book chapters on these topics. He also has many years of teaching experience on these topics.

Lieutenant Colonel Michael Navicky, USAF (Ret.), is deputy director of the High-Performance Computing Collaboratory at Mississippi State University, where he oversees computing, data storage, data communications, and general operations. Mississippi State University houses the sixth fastest supercomputer in academia along with four other supercomputing clusters. This computational power supports research in artificial intelligence, autonomous vehicles, cybersecurity, data science, weather modeling, and other areas of applied research. His current research focuses on the collection, exploitation, and visualization of publicly available information.

Prior to joining the Mississippi State University team in June 2021, Lieutenant Colonel Navicky served 21 years in the U.S. Air Force. During this time, he logged more than 3,000 flight hours in the C-17, MQ-1, and MQ-9. The highlight of his aviation assignments was his year in Kandahar, Afghanistan, serving as the commander of the Air Force's largest launch and recovery MQ-1/9 squadron. In 2016, Lieutenant Colonel Navicky transitioned into cybersecurity, serving to develop cybersecurity policy during his assignment at the Pentagon in the Secretary of the Air Force/Chief Information Officer A6. Additionally, he served as the commander of a 110-Airmen communications squadron providing network services for 6,000 users. Lieutenant Colonel Navicky is a 2018 graduate of the U.S. Army War College.

Dr. Benjamin Tkach is an assistant professor of political science in the Department of Political Science and Public Administration at Mississippi State University, where he teaches international relations. He previously held a position at King University and held a post-doctoral fellowship sponsored by the U.S. Agency for International Development (USAID) at the Center on Conflict and Development at Texas A&M University. He has collaborated with the National Defense University, Joint Special Operations University,

and the Department of Energy. His primary research agenda investigates government decentralization, security privatization, and nonstate actor involvement in conflict processes. He adopts a broad theoretical conceptualization of government decentralization that encompasses governance at multiple levels (national and international) and conceptualizes decentralization as shifts from public to private provision of security. His research has been supported by Mississippi State University's Office of Research and Economic Development and the Office of Institutional Diversity and Inclusion, Joint Special Operations University, and USAID.

Dr. Tkach's research has appeared in *Conflict Management and Peace Science*; *Information, Communication, and Society*; *International Peacekeeping*; *International Interactions*; *Peace Economics, Peace Science and Public Policy*; and *Public Administration*.

Mr. J.D. Work is a professor in CIC at NDU. His research focuses on cyber intelligence, operational art, and strategy in conflict and competition. Mr. Work has over 25 years' experience working in cyber, intelligence, and operations roles for the private sector and U.S. Government. He holds additional affiliations with the Saltzman Institute of War and Peace Studies at the School of International and Public Affairs at Columbia University, the Krulak Center for Innovation and Future Warfare at the Marine Corps University, and the Cyber Statecraft Initiative at the Atlantic Council.


NDU
Press