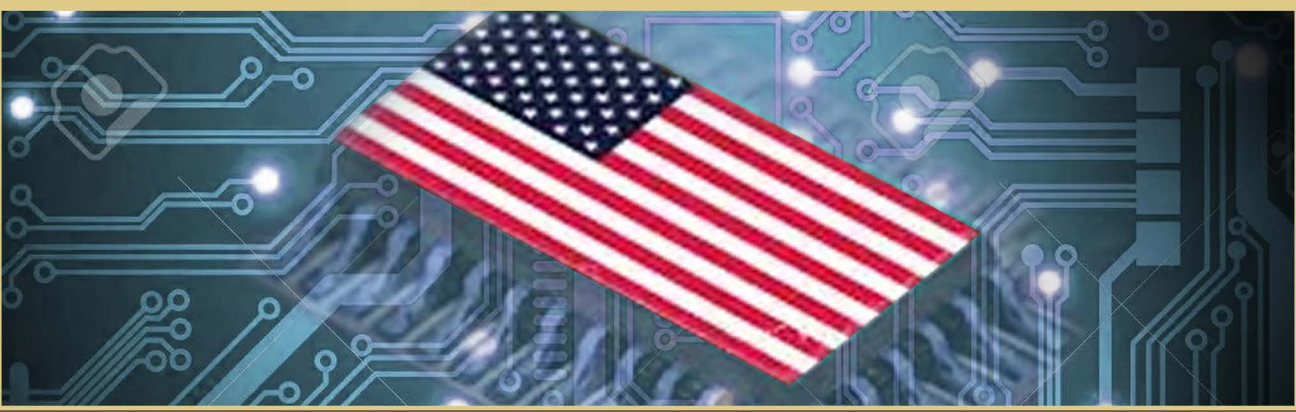
PERSPECTIVES ON CYBER POWER

CPP-8

Cyber Deterrence Revisited

STEFAN SOESANTO



AIR UNIVERSITY

AIR UNIVERSITY PRESS

Cyber Deterrence Revisited

Stefan Soesanto

CPP-8

Air University Press
Academic Services
Maxwell Air Force Base, Alabama

Director, Air University Press
Dr. Paul Hoffman

Project Editor
Jeanne K. Shamburger

Illustrators
Catherine Smith
Timothy Thomas

Printing Specialist
Nedra Looney

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://www.facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Accepted by Air University Press October 2021 and published April 2022.

ISSN 2831-5251

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors and do not necessarily represent the official policy or position of the organizations with which they are associated or the views of the Air University Press, Air University, United States Air Force, Department of Defense, or any other US government agency. This publication is cleared for public release and unlimited distribution.

AIR UNIVERSITY PRESS

Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Cyber Papers are available via the AU Press website at https://www.airuniversity.af.edu/AUPress/.

Contents

About the Author *v*

Abstract *vi*

The Rise and Death of Cyber Deterrence 1

Cyber Deterrence Theory or Causal Expectations? 3

Cyber Deterrence Theory? 6

Cyber Deterrence Mechanisms 7

- Deterrence by Denial 8
- Deterrence by Delegitimization 9
- Deterrence by Punishment 10
- Deterrence by Entanglement 13
- Deterrence by Reputation 14
- Cross-Domain Deterrence 17

When Is Cyber Deterrence Successful? 20

When Is Cyber Deterrence Unsuccessful? 22

Further Thoughts 24

Conclusion 26

Abbreviations 32

Bibliography 33

About the Author

Stefan Soesanto is a senior cyber defense researcher at the Center for Security Studies (CSS), ETH Zürich, Switzerland, currently working on the Cyberdefense Project with the Risk and Resilience Team. Prior to joining the CSS, he was the Cybersecurity and Defense Fellow at the European Council on Foreign Relations (ECFR) and a nonresident James A. Kelly Fellow at Pacific Forum, Center for Strategic and International Studies. At ECFR, he designed and held cyber wargame exercises in cooperation with Microsoft and organized a closed Cybersecurity and Defense conference in Denmark together with the Center for War Studies at the University of Southern Denmark and the Office of the Danish Tech Ambassador. Mr. Soesanto also served as a research assistant at RAND's Brussels office, coauthoring reports for the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Network Information Security Agency (ENISA), and Dutch Ministry of Security and Justice. Stefan holds a master of arts degree from Yonsei University (South Korea) with a focus on security policies and international law and a bachelor of arts degree from Ruhr University Bochum (Germany) in political science and Japanese. You may contact him at stefan.soesanto@sipo.gess.ethz.ch.

Abstract

The discourse on cyber deterrence is a melting pot of ideas, concepts, and experiments meant to continuously twist, bend, and refine our understanding, from the conflict dynamics playing out in cyberspace to the psychological deterrence effects taking root inside the human mind. At least, that is how it ought to be. With the exception of persistent engagement, cyber deterrence thinking has to a large degree treaded intellectual water due to the absence of access to operational data and insights into the tactical decision-making processes. To circumvent this substantial gap, academics have turned to recycling and transposing known deterrence mechanisms onto the cyber domain to mimic known behavioral outcomes elsewhere. Overall, those efforts have had limited practical success or could even be considered counterproductive for creating a deterrence theory applicable to cyberspace. This paper is a correcting effort to disentangle the ongoing academic discussions. It critically reflects on mechanism outcomes, shortfalls, and misconceptions and explains when cyber deterrence is successful and when it is not. It also outlines potential research avenues, policies, and access requirements that will likely help to ascertain the deterrence effects we so desperately crave to create in cyberspace.

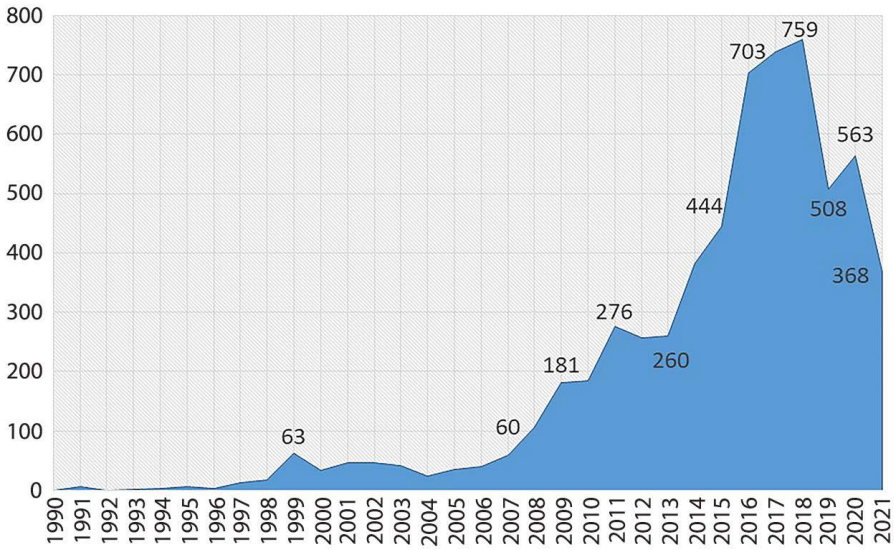
The Rise and Death of Cyber Deterrence

Twenty-five years ago, James Der Derian, now director of the Centre for International Security Studies at the University of Sydney, coined the term *cyber deterrence* in his 1994 *Wired* piece on the US Army's Desert Hammer VI war-game exercise.[1] But far from outlining "how an adversary can be deterred in cyberspace," Der Derian's term described the Army's fusing of "media voyeurism, technological exhibitionism, and strategic simulations" for creating a hyper-digitalized image of US military dominance across the three traditional war-fighting domains.[2] In the aftermath of Desert Storm—which saw the baptizing of stealth technology, precision-guided ammunition, and the unprecedented access of embedded journalists in combat operations—this definition of cyber deterrence made perfect sense, as deterrence logics are fundamentally intertwined with human psychology.

Fast-forward 25 years and *cyber deterrence*—like many other cyber terms—has an entirely different meaning. Today, it predominately describes a wide array of meatspace (physical world) theories and mechanisms that were transposed into the cyber domain, including long-standing international relations theories, criminological methodologies, and techniques inherent to psychological warfare. Der Derian's original definition presently rests in the latter category, so far receiving little recognition within the wider field of cyber deterrence research.

It is unclear when exactly the academic discussion on deterring adversaries in cyberspace fermented. As far as the literature is concerned, the bulk of journal articles, book chapters, and research reports on the specific terms "cyber deterrence/cyberdeterrence" emerged during the Kosovo conflict in 1998–99, with a rapid increase after the distributed denial-of-service (DDoS) attacks against Estonia in 2007 (fig. 1).

Yet, looking at the technical dynamics underlying the concept of conflict in cyberspace, various aspects now inherent to the thinking on cyber deterrence have always been closely linked to continuous software and hardware developments, the expanding reach of the internet, and the evolution of the World Wide Web. Thus, while cyber deterrence as a strategic concept may not have existed in name prior to 1994, its elements featured prominently in practice—starting in the 1970s with the first self-propagating worm (Creeper) that was killed by a worm (Reaper) and the rise of the antivirus software industry in the mid-1980s.[3]



[a]Annual JSTOR search results for the terms "cyber deterrence," "cyberdeterrence," and "cyber" and "deterrence." During the write-up of this paper, JSTOR improved its search algorithm, so it is now possible to search for the exact term "cyber deterrence" when put in quotation marks. This was previously not possible. The logic of including the search results for "cyber" and "deterrence" was derived from also trying to capture sentences and logical connections over several pages that touch upon cyber deterrence without specifically using the words "cyber deterrence" or "cyberdeterrence." The annual division was attained by searching for the keywords from 2000/01 to 2000/12 (year/month). Additionally, the search was performed with the "access type" switched to "all content" to capture even those publications JSTOR includes in its search results that are inaccessible through the JSTOR subscription. The methodology has several shortcomings, which, although significant, the author deems sufficient for estimating the growth and decline of the usage of the terms "cyber deterrence" and "cyberdeterrence."

Figure 1. Journal articles, book chapters, and research reports on "cyber deterrence," "cyberdeterrence," and "cyber" and "deterrence" (as of January 2022)

Overall, the strategic discussions on cyber deterrence were—and still are—largely hindered by the absence of military-to-military conflict in cyberspace.[4] As a case in point, activities in cyberspace during the 1998–99 Kosovo conflict—widely anointed as the first "Internet war"—were entirely "fought" by patriotic hackers targeting NATO government officials with malware-ridden emails, conducting DDoS attacks against NATO email servers, and defacing US government websites.[5] During the same time frame, the FBI's investigation into the Russian-linked Operation Moonlight Maze also kicked off the "dawn of nation-state digital espionage," as characterized by Kaspersky Lab.[6] In both instances, cyber deterrence took shape in the form of incident mitigation, then the sole responsibility of system administrators, and cybercriminal investigations, severely hindered at the time by analytical hurdles and legal constraints in tackling cross-border crime. The militarization of

cyberspace—and with it, cyber deterrence as currently envisioned by defense planners and military strategists—gradually developed in reaction to the increasing number and severity of advanced persistent threat (APT) actor campaigns.[7] Hence, the concept of cyber deterrence as it is now understood likely originated sometime between 2006—when the term APT was coined by Greg Rattray—and the DDoS attacks against Estonia in 2007.[8]

Figure 1 pinpoints that the academic discussion on cyber deterrence accelerated around 2007 and peaked 11 years later with 759 publications in 2018. Scholarly output on the topic rapidly declined in the following years to the extent that in 2021, only 368 journal articles, book chapters, and research reports discussed cyber deterrence. To some degree, the academic death of cyber deterrence echoes the rise of the concept of persistent engagement, whose theoretical foundations were laid by Richard Harknett and Emily Goldman in 2016.[9] However, to a much larger degree, the academic discussion on cyber deterrence has effectively been treading intellectual water for the past decade in substance and functional output.[10]

Cyber Deterrence Theory or Causal Expectations?

The discourse on cyber deterrence can be roughly divided into two parts: identifying deterrence aims and highlighting ways and means of achieving them. Within this field, academic research centers on the feasibility of strategic deterrence through the application of international relations theories to the cyber domain. That is, it generally does not touch upon the operational art of cyber, such as how militaries defend, fight, and win in cyberspace.[11] To a large extent, academia cannot be blamed for this blind spot. Militaries everywhere have done a poor job of engaging the academic community on the topic of cyber deterrence to begin with. In most instances, this nonengagement is due to (1) military leaders not knowing if cyber deterrence is a workable concept, (2) the highly classified nature of the operational art of cyber, and (3) the likelihood that deterrence tactics are built from the bottom up versus from the top down, as the technical expertise resides with the operators sitting in front of the keyboard and not the military brass.

Over the past decade, this technical disconnect has resulted in two foundational academic discussions that remain unresolved. First, is cyber war in its strictly violent form possible? And second, is strategic signaling in cyberspace as a central element of deterrence feasible?[12] On both issues, the classified nature of offensive cyber operations and the lack of comprehensive case studies on the topic have resulted in the rather awkward situation that academics

overwhelmingly react to developments in cyberspace rather than conceptually leaping ahead of them.

Another downside to the dominance of international relations thinking in the field is the creation of several underdeveloped cyber deterrence research silos that encapsulate distinctly different views, such as the fields of criminology (deterring cybercrime), psychology (deterring information warfare), intelligence studies (deterring cyber espionage), and computer sciences (deterring network disruptions). This fragmentation has led Aaron F. Brantly, assistant professor in the Department of Political Science at Virginia Polytech and State University, to argue that the main challenge is not defining deterrence in cyberspace but "understand[ing] the role digital technologies play in the broader scope of interstate deterrence."[13]

If Brantly is right, then academia must resolve one fundamental question: Are the discussions on cyber deterrence based on sound theoretical thought emanating from knowledge and experimentation gathered from inside the cyber domain, or are we merely transposing deterrence mechanisms onto the cyber domain to mimic known behavioral outcomes elsewhere? Specifically, if cyber deterrence theories substantially borrow from outside the cyber domain, then are they really "cyber" theories?

For military planners and strategists, this question might seem irrelevant because "deterrence has always been widely practiced against all potential threats to state interests as a matter of necessity."[14] But for academics, understanding how, why, and when deterrence works is an evolutionary process. As Robert Jervis indicated in 1979, "good theories do not spring full-blown from the minds of a few scholars. Rather, they develop as people test them and examine their internal dynamics and causal linkages."[15] Deterrence theory itself is probably the best example to showcase this process, as it has evolved along at least four distinctive research waves—with a fifth one emerging. The first wave kicked off immediately after World War II when the strategic implications of nuclear weapons became apparent. The second wave was deeply engrained in game theory and bargaining tactics to gain insights into "the ways an actor manipulates threats to harm others in order to coerce them into doing what he desires."[16] Starting in the 1970s, the third wave filled the largely deductive theories of the previous waves with statistical and case study methods to empirically test deterrence theory, stressing that it "needed to be modified with regard to risk taking, rewards, probabilities, misperceptions, and domestic and bureaucratic politics."[17] The fourth wave accelerated after 9/11 and, according to Jeffrey Knopf, reflected "a change from a focus on relatively symmetrical situations of mutual deterrence to a greater concern with what have come to be called asymmetric threats"—including terrorism, rogue states,

and cyberspace operations.[18] The fifth and latest research wave, still in its embryonic stage, centers on the concept of resilience to deter and cope with the myriad complex, networked, and distributed security threats in today's globalized world.[19]

Now, cyber deterrence as a theory languishes between the first and second waves due to the absence of large empirical data sets, comprehensive case studies, and substantial play-by-play technical insights. Consequently, the academic discussions on cyber deterrence are overwhelmingly deductive, reductive, and superficial and have led to a range of arguments. These include deterrence in cyberspace does not exist, it has more in common with preventing cybercrime, it necessitates continuous persistent engagement wherever the adversary moves, and it can work only in the context of a "whole of government" approach that also comprises sanctions, indictments, and diplomatic démarches.[20]

On the other hand, cyber deterrence as a mechanism is inherent to the fourth and fifth deterrence waves. That is, it is rooted in the wealth of knowledge emerging from traditional deterrence theory and thus, according to international relations theorists, needs only to be adapted and refined to the new challenges of today. Cyber deterrence mechanisms therefore do not necessitate the creation of an entirely new deterrence theory, nor do theorists recognize cyberspace as a unique domain. Consequently, within the fourth wave, cyber deterrence is closely aligned with the question of how to deter terrorism. This connection led Uri Tor to adapt the idea of cumulative deterrence to cyberspace by mirroring the Israeli experience in fighting violent extremist organizations.[21]

Meanwhile, in the context of the fifth wave, cyber deterrence mechanisms align closely with the cybersecurity paradigm of resilience, for example, preparing for compromise and defending in-depth rather than focusing on perimeter defense. However, if recovery and defending inside a network are used to essentially absorb an attack, then the original premise of deterrence—coercion and discouraging an attack—is left unfulfilled. Resilience does not tackle the original deterrence problem of why a system or network was targeted, infected, and breached. Nevertheless, a resilient network might under certain circumstances create deterrence effects, particularly if the same adversary is tasked to breach the same network again (repetition). But even a resilient network is unlikely to deter the exfiltration of sensitive data, temporary network disruption, or campaigns aimed at physical destruction.

As far as this author is concerned, cyber deterrence theory and its continuous development currently exist only at the tactical and operational levels. Operators are still experimenting with what does and doesn't work in terms

of developing capability, creating and controlling fires and effects, signaling, determining adversarial courses of action (i.e., shaping behavior), and so forth. Cyber deterrence mechanisms, conversely, are an integral part of the strategic-level discussions pertaining to controlling conflict and maintaining stability in a multi-domain world. Thus, the fundamental barrier to progress in cyber deterrence research is the absence of insights into the evolution of thought and ideas at the operational level for the sake of connecting the strategic decision-making process with the tactical and operational actions taken in cyberspace and vice versa. While this gap persists, the discussions on cyber deterrence will stall and likely veer increasingly into the wrong direction due to inadequate evidence and poor analysis that might result in ineffective—if not even counterproductive—outcomes down the road.

The academic field is already struggling with elemental knowledge problems. They include analytical outputs derived from low-quality cyber conflict databases; n-studies conducted with non-operators to map and predict escalation dynamics; DDoS, phishing emails, and pings misclassified as cyber-attacks; and exploits mischaracterized as cyber weapons. If cyber deterrence becomes an integral part of this already long list, then policy makers and military planners could make decisions based on fundamental theoretical misunderstandings and misconceptions. It is our task to stem the tide and prevent this outcome. This paper is part of that correcting effort.

Cyber Deterrence Theory?

So far, one question looms large above the entire cyber deterrence debate in the field of international relations. Can cyber deterrence theory exist without a clear understanding of what distinct adversarial activities governments seek to deter in the first place? For instance, should they deter DDoS attacks, ransomware campaigns, and cyber espionage efforts? Or should only activities that create a significant effect synonymous to an armed attack be deterred? If we extend this question further, we need to ask whether these adversarial activities ought to be separated along nation-state conduct, non-nation state conduct, and the varying degrees of relationship, control, and mission tasking that exist between state and non-state entities and individuals. Yet the further we go down this road, the blurrier the dividing lines become. In the end, we are left with only one choice: deter everything—no matter what, no matter who, no matter where.

This approach is synonymous with how law enforcement is combatting cybercrime. Practical deterrence mechanisms include everything from raising awareness and providing alternative career paths to first offenders to law

enforcement posting threatening messages on hacker forums, breaching the infrastructure of cybercriminal networks, and conducting coordinated global takedown operations against organized cybercriminal groups.[22] Fundamentally, though, law enforcement does not engage in a detailed discussion about whether carding, ransomware, or business email compromise campaigns should be deterred or whether there is a level of cybercriminal activity that should go undeterred. All criminal activities fall into the remit of law enforcement and must be deterred. The luxury of choice does not—or should not—exist. Therefore, for law enforcement, the question is not whether cybercrime can be deterred— which largely goes unquestioned—but how to deter it more effectively, holistically, and persistently across all accessible jurisdictions.

Notwithstanding, even Europol notes in its *Serious and Organised Crime Threat Assessment* (SOCTA) 2021 that "the experience[s] of law enforcement authorities have shown that even successful and far-reaching disruption of criminal networks has little long-term consequence for the overall activities of organised crime."[23] Other research silos have—as of this writing—shied away from reaching this inevitable conclusion. The field of intelligence studies, for example, is still undecided about whether cyber espionage should and can be deterred. Even further behind is the field of psychology, so far entirely avoiding a discussion of whether information warfare (i.e., disinformation and propaganda campaigns) should and can be deterred at all.

And yet while the overarching question as to what adversarial activities we want to and should deter remains crucial, it is and will always be a matter of policy and politics and not deterrence theory. The only question a cyber deterrence theory in the field of international relations ought to concern itself with is this: Does deterrence work in and through cyberspace? As of this writing, this question has not been fully investigated to produce a definite answer. Speaking at the Aspen Security Forum 2021, Gen Paul Nakasone, USA, head of US Cyber Command, stated that traditional military deterrence "is a model that does not comport to cyberspace."[24] However, he also stressed that "we are still a learning organization. How the deterrence model is going to play out and how much of the competition space influences what adversaries are doing . . . we are still learning."[25]

Cyber Deterrence Mechanisms

Despite the academic shortcoming on the theory side, six deterrence mechanisms (not theories) have emerged over the years that have been trying to influence and outline the underlying dynamics for how deterrence in cyberspace might work in practice.[26] These are (1) deterrence by denial, (2) deterrence

by delegitimization, (3) deterrence by punishment, (4) deterrence by entanglement, (5) deterrence by reputation, and (6) cross-domain deterrence.

Deterrence by Denial

Deterrence by denial is the earliest and most basic mechanism for deterring adversaries in cyberspace. It largely rests on the field of cybersecurity, encompassing defining and implementing security standards, segregating networks, constantly monitoring traffic, and enhancing "an organization's ability to maintain, change or recover technology-dependent operational capability."[27] The overall aim of deterrence by denial is to decrease an attacker's probability of success by reducing a system's attack surface and limiting an adversary's breakout time and lateral movement within a network. Concerning international relations theory, deterrence by denial centers on disrupting an adversary's cost-benefit calculation to the degree that it either disincentivizes an attack due to the increased likelihood of failure or the subsequent exhaustion of an attacker's time, patience, and/or resources.[28] Deterrence by denial primarily differs from cybersecurity in that the former is a mechanism of strategic signaling while the latter is a societal need in line with the increasing reliance on technology.

The first problem with applying deterrence by denial to the cyber domain is that adversaries across the threat spectrum likely calculate cost-benefits differently over space and time—if calculating them at all. These adversarial differences can stem from capability and capacity considerations, the level of organizational maturity, mission success requirements, targeted or general fire and effects, and a host of other factors that constrain, define, and characterize adversarial behavior.[29] The same cost-benefit problem likewise exists on the other end, with network defenders having a hard time quantifying the cost-benefit of each cybersecurity action taken. Gerald Willard, senior technical leader at the National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center, assessed that "in the cybersecurity world there are almost always tradeoffs," but "most network defenders believe that all security measures result in good consequences."[30] However, outcomes can include securing a network to the degree that users search for loopholes and work-arounds to make their life easier; anti-phishing training and email filters provide a false sense of trust, knowledge, and expertise; and users believe that the features and technologies of the latest upgrade install will eliminate misconfigurations debt, legacy debt, and a larger attack surface.[31] Cultural differences also come to play in prudently securing a system. Robert M. Lee, CEO of Dragos, delineates the cultural differences between information

technology (IT) and operational technology (OT): "When the IT security people come in, the first thing they want to do is patch a system when they really should be asking why. What am I trying to derive value on? What risk am I trying to reduce? Patching has taken down more oil and power sites than Iran, China, and Russia combined."[32]

From a causal relationship point of view, it is also questionable whether a secure system—say an air-gapped laptop stored behind walls and walls of steel-reinforced concrete—deters anyone or adversely attracts the most persistent and skilled attackers. The available data does not show a correlation between cybersecurity investment and the number or probability of breaches. In essence, nobody knows how to achieve a reasonable return on investment or has any idea of how much to spend on cybersecurity.[33] Overall, the sheer dynamics and complexity of constantly protecting changing systems, networks, programs, and supply chains against an infinite number of vulnerabilities and evolving attack vectors is staggeringly difficult—if not impossible—to achieve in a globalized world. Generally, deterrence by denial works best for sparsely populated nation-states with a minimal digital footprint that are largely disconnected from the outside world (e.g., North Korea) and are de facto unattainable for densely populated, highly digitalized countries at the epicenter of the technological revolution (e.g., US, China). In a similar vein, RAND's Martin Libicki observed a decade ago that "none of this says that defenses are pointless, but claims that they may discourage cyberattack attempts need to be viewed cautiously."[34]

Deterrence by Delegitimization

Deterrence by delegitimization, also known as naming and shaming, has its wider origin in the governmental deliberations on creating norms and rules for state behavior in cyberspace (e.g., UN's Group of Governmental Experts [GGE] and Open-Ended Working Group [OEWG]) and the academic discussions on the applicability of international law to the cyber domain (e.g., the two *Tallinn Manuals*). The overall aim of this process is threefold: create a general principle of restraint, raise the reputational costs of bad behavior, and shrink the battlespace to encompass only military combatants in line with the law of armed conflict. While numerous states and international organizations have been pushing this narrative for more than a decade, only a handful of governments have publicly attributed normative violations of international law to a particular individual, group, or nation-state. As it currently stands, the Five Eyes are the predominant countries to have engaged in coordinated public attribution behavior. Notably, they called out Russian military intelligence

for the NotPetya campaign and the close hacking operation against the Organisation for the Prohibition of Chemical Weapons (OPCW) (in cooperation with the Dutch government). They also blamed the Chinese Ministry of State Security for the APT10 and APT40 campaigns in 2018 and 2021, respectively (in cooperation with the Japanese government).[35] According to the interpretation of the Five Eyes, public attribution yields overall positive returns with attackers "sometimes" altering their behavior.[36] Indeed, the overwhelming majority of APTs refine their tactics, techniques, and procedures when exposed to the public, and some even opt to share parts of their tooling and infrastructure with other groups to muddy the waters and confuse defenders. But so far, only one threat actor—APT3/Boyusec—has entirely vanished after being doxed in April and May 2017 by the anonymous group known as Intrusions Truth.[37] In fact, the most resounding success in public attribution has not been the result of a coordinated diplomatic push at the international level or a multilateral effort by the Five Eyes but of a non-state actor likely fed up with the all too cautious and slow government public attribution efforts.

Deterrence by Punishment

Despite being the most widely discussed approach, the concept of deterrence by punishment is still in its infancy in theory and practice. If we accept the logic of the *Tallinn Manual* and the discussions on norms in cyberspace related to offensive cyber operations, then deterrence by punishment is only acceptable if leveraged in self-defense in reaction to a nation-state cyber operation that resulted—or is expected to result—in severe harm.[38] Subsequently, when the attack is confidently attributed to another state, "the victim state may respond forcefully in self-defense [within a proximate temporal range] so long as doing so is consistent with the criteria of necessity and proportionality."[39] In theory, deterrence by punishment is fraught with all kinds of nit-picky problems that essentially make it impractical for a defender to respond appropriately. These include the prioritization of immediate incident remediation over concerns of attribution, the inherent uncertainty of the initial attribution assessments, and conflicting interpretations of the meaning of proportionality, distinction, necessity, humanity, and military advantage in the military targeting process for cyberattack response.

In practice, however, deterrence by punishment comes down to one simple thing: "You hurt me, I'm going to hurt you worse. I have the tools to do it, and if you don't believe me, then step over the line," as stated by Gen Paul J. Selva, former vice chairman of the Joint Chiefs of Staff.[40] The discrepancy between these two lines of thought encapsulates the persisting political and legal friction

between the question of how a state would have to respond to avoid escalation in cyberspace (i.e., respecting legal parameters and trying to maintain overall stability) versus how a state would like to respond to deter in cyberspace (i.e., disproportionally, imposing dominance to avoid creating an escalation ladder). Given the few examples of offensive military cyber operations that have caused serious harm and would illicit an armed response, academic research on controlling escalation dynamics in cyberspace is largely still theory driven and error prone. Herb Lin at Stanford's Center for International Security and Cooperation summarized the situation aptly when he noted that "although existing theories of escalation dynamics and conflict termination may serve as useful points of departure, what is understood very poorly today is how these theories may apply in cyberspace."[41]

In defiance to the uncertainties surrounding escalation dynamics, Harknett and Goldman argued in 2016 that cyberspace is an offense-persistent strategic environment. That is, "the defense cannot win strategically alone; at best, the contest will result in a draw. The defense can achieve tactical and operational success, but the offense will persist, the contact with the enemy will remain constant, and the defense will need to adjust as the terrain to defend and the vectors to attack evolve."[42] One year later, Harknett and Fischerkeller made the case for persistent engagement in that "the cyberspace operational domain calls for a strategy of cyber persistence, a strategy based upon the use of [cyber operations, activities, and actions] (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in cyberspace so that the United States could ultimately deliver direct effects in, through, and from cyberspace at a time and place of its choosing."[43] In 2018, US Cyber Command (USCC) essentially adopted the logics of persistent engagement through its endorsement of the concept of defending forward by declaring that "superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver."[44]

Since then, USCC and the NSA have embarked on tactical avenues to operationalize persistent engagement. One of those publicly known endeavors is Operation Synthetic Theology, which included directly messaging operatives working for Russian military intelligence and temporarily disrupting the Internet Research Agency (IRA) in the run-up to the 2018 US midterm elections.[45] Another is an operation against Trickbot that poisoned the configuration files on its command-and-control servers in an effort to reduce its potential impact on the 2020 US presidential election.[46] General Nakasone also testified before the Senate Armed Services Committee that US Cyber Command

conducted "more than two dozen" operations to counter foreign attempts to interfere with or influence the 2020 elections.[47] As of this writing, it is unclear whether other USCC operations fall under the umbrella of persistent engagement as well. One example is USCC's operation in June 2019 against an "Iranian intelligence group that American officials believe helped plan the attacks against oil tankers," an operation in September 2019 that took aim at Tehran's ability to spread propaganda and supposedly affected physical hardware. Another instance is USCC's offensive operation in September 2021 against the Russia-based REvil ransomware group in the aftermath of the attacks against Colonial Pipeline and JBS beef plants.[48] Overall, the publicly known USCC operations paint a picture of targeted engagements timed to disrupt or halt an expected or ongoing adversarial campaign. This strategy stands in stark contrast to the theoretical objective of persistent engagement, which aims to continuously engage and contest adversaries to create uncertainty wherever they maneuver.

Another confusing point that needs clarification is the case Harknett and Fischerkeller make for persistent engagement because "deterrence is not a credible strategy for cyberspace" due to the "domain's unique characteristics."[49] Yet the 2020 US Cyberspace Solarium Commission has advocated for a new strategic approach it calls "layered cyber deterrence," which in the commission's own words fundamentally builds on defend forward—a "posture impl[ying] persistent engagement with adversaries as part of an overall integrated effort to apply every authority, access, and capability possible to the defense of cyberspace in a manner consistent with international law."[50] Commission members have largely glossed over the obvious tension of including persistent engagement in a national cyber deterrence strategy by shifting the focus to authorities, accesses, and capabilities or, in other words, deterrence mechanisms.[51]

Fitting into this confusion is the 2021 paper "Deterrence by Denial in Cyberspace" by Erica Borghard and Shawn Lonergan. It makes the case that deterrence by denial comprises two components: denial and defense. The defense component is purely defensive, and the denial component is geared toward denying an adversary battlefield success. Taking the denial component, Borghard and Lonergan then proceed to build an argument for a deterrence by denial posture that fundamentally hinges on conducting "counter-cyber operations that target adversary offensive cyber capabilities and the infrastructure and organizations that enable it."[52] As Borghard and Lonergan themselves admit, "the DoD's concept of defend forward is the closest allegory in practice to this approach to denial."[53] Curiously though, while Borghard and Lonergan note that persistent engagement threw "the deter-

rence baby out with the bathwater," they omit that defend forward is fundamentally based on persistent enagagement to begin with.[54]

Lastly, it is unclear whether, theoretically, persistent engagement can mimic long-term deterrence effects as a side product. As it stands, the IRA and Trickbot regenerated, and Iran likely also regenerated its capabilities in the aftermath of USCC's operations.[55] From the public evidence available, it is uncertain whether USCC's operations had a deterrent effect—or maybe created enmity as a counterproductive result—and to what degree USCC's activities were able to shape adversarial behavior and thinking.

Deterrence by Entanglement

Deterrence by entanglement was most prominently articulated by Joseph Nye in his 2017 paper "Deterrence and Dissuasion in Cyberspace."[56] The theory of entanglement rests largely on the unresolved international relations discussions as to whether state-to-state interdependencies facilitate or mitigate interstate conflict.[57] Nye posits that within the broader framework of cyber deterrence, a strategy of entanglement would simultaneously impose serious costs on the attacker and the victim. Leveraged in practice, a state would thus seek to "enhance benefits such that it creates a disincentive and minimizes risk seeking by an adversary."[58]

The fundamental problem with entanglement is that there is currently no example that would support its applicability to the dynamics in cyberspace. The Snowden revelations show that long-standing allies spy on each no matter their interdependencies elsewhere.[59] Existing economic interdependencies between the US and China also did not prevent the rapid collapse of the 2015 Obama-Xi agreement. According to the APT40 indictment, "approximately one month after China's President committed to the United States that its government would not conduct or knowingly support cyber-enabled theft of intellectual property . . . , members of the conspiracy installed PHOTO malware on a system operated by [an aircraft servicing company headquartered in New Jersey] and later stole proprietary data related to fire-suppression systems and other data."[60] In April 2018, Adm Philip Davidson, head of US Indo-Pacific Command, stated that Beijing was snatching anything not nailed down—"stealing technology in just about every domain and trying to use it to their advantage."[61] By November that year, the Obama-Xi agreement was effectively dead.[62] According to Priscilla Moriuchi, former lead of NSA's East Asia and Pacific cyber threats office, it was unclear whether China ever really took its commitments under the agreement seriously.[63]

Equally, the deployment of Triton against Saudi Arabia's Petro Rabigh oil refinery in 2017 undermines the deterrence by entanglement logic.[64] Dubbed "the world's most murderous malware" by *MIT Technology Review*, Triton was specifically designed to disable the protection systems of industrial control systems to facilitate physical accidents and bodily harm.[65] In October 2018, security firm FireEye assessed with "high confidence that intrusion activity that led to deployment of TRITON was supported by the Central Scientific Research Institute of Chemistry and Mechanics, a Russian government-owned technical research institution located in Moscow."[66] Yet, while Moscow deployed Triton against the Kingdom and Western countries shunned Saudi Arabia over the brutal murder of *Washington Post* columnist Jamal Khashoggi, it also sent a Russian trade delegation of 30 top executives to participate in the Kingdom's "Davos of the Desert" investment conference. As Russian president Vladimir Putin proclaimed at the time, "in truth, we do not know what happened [with Jamal Khashoggi]. . . . So why should we take any steps that could harm our relations with Saudi Arabia?"[67] Talking to *Wired*, Andrea Kendall-Taylor, former deputy national intelligence officer for Russia and Eurasia at the Office of the Director of National Intelligence (ODNI), asserted that "Moscow's targeting of Saudi Arabia is inconsistent with my understanding of Russia's geopolitical goals."[68]

In a more recent example, Crowdstrike detected activities of hackers with suspected links to the North Korean regime (i.e., Lazarus/Stardust Chollima) targeting Chinese security researchers "in an apparent attempt to steal their hacking techniques and use them as their own."[69] Beijing and Pyongyang have had a defensive alliance treaty since 1961—the only defense treaty China and North Korea have with any country—and friendly economic relations with Beijing remain vital to the survival of the North Korean regime. Accordingly, one ought to seriously question whether even Beijing would buy into Nye's assertion that entanglement in cyberspace is a workable concept.[70]

In the end, all four examples outlined above are bound only by simple logic: no matter the level of entanglement in real space, there are no friends in cyberspace.

Deterrence by Reputation

Deterrence by reputation is a well-established concept in traditional deterrence theory but is rarely, if ever, covered in the context of cyberspace. In his 1966 work *Arms and Influence*, Thomas Schelling makes the contentious argument that a country's image "is one of the few things worth fighting over . . . [because] it is a country's reputation for action, the expectations other coun-

tries have about its behavior."[71] That is, reputation and the resolve to deter are formed through past-iterated encounters—and the expectation of future crises—between the same two actors.

In the context of the cyber domain, the US, for example, threw down the gauntlet at Iran in 2009 with the deployment of Stuxnet against the nuclear facility in Natanz. Similarly, the Russian Federation drastically reshaped its own image with the intrusion into the Democratic National Convention (DNC) and the subsequent information warfare campaign against the 2016 US presidential election. In terms of deterrence by reputation, the US government clearly conveyed the message that its intelligence agencies are sophisticated and could infect and physically damage any system no matter how deeply it was buried underground—technically, nothing was out Washington's reach. If Iran wanted to compete with the US on these terms, it was surely destined to fail—or so the story goes. The Russian government in turn proved it could run a successful information warfare campaign against the only remaining military superpower and get away with it. Moscow's reputation was subsequently hyped to such an extent that its information warfare capabilities were seen as almost magical powers able to influence anything, anywhere, for pennies and nickels. In terms of deterrence by reputation, Moscow clearly signaled to Washington its asymmetric superiority in the information warfare space and the willingness to use its capabilities offensively to destabilize societies and political systems during peacetime. As Libicki explained, "As long as other countries believe we can do magic, what we can actually do matters less for deterrence purposes."[72]

Yet, to date, few research efforts have been made to deepen our understanding about whether reputational aspects reinforce defensive behavioral choices or self-restrain offensive actions in cyberspace. For instance, has the NSA's Tailored Access Operation team developed a self-image that now results in running sophisticated attacks against targets although simpler measures would achieve the same results? And similarly, for the Iranian side, has the US reputation in cyberspace deterred or reinforced Tehran's efforts to measure up to the US offensively or better defend themselves at home? Answers to both questions are likely found at the tactical and operational, not strategic, levels. Thus far, we have no substantial insights into how operators adapt to new attack vectors and sophisticated malware code popping up in the wild. We also do not fully grasp whether they respect foreign adversarial teams or how much psychology is a factor when teams run their campaigns against foreign government targets. To this author, it seems that on an academic level, the strategic view persists that cyber operations happen in a clean, orderly environment without any emotions involved when most likely the opposite is

true. Cyber operations are messy, operators become frustrated, and things usually never go according to plan. More research is needed to understand these internal dynamics and the reputational effects that teams can create and leverage over time when operating outside their own wire.

One example that likely affects deterrence by reputation dynamics and probably plays an increasing role in making deterrence by denial viable is the uploading of adversarial malware samples onto community platforms like Virus Total.[73] US Cyber Command, or more specifically the Cyber National Mission Force (CNMF), started this initiative on November 5, 2018, to engage the information security community quickly, simply, and noncontextually to bolster private-sector defenses against adversaries.[74] John Hultquist, director of Intelligence Analysis at FireEye, stated, "What is striking about this initiative is it lacks many of the contextual elements of the name and shame strategy [i.e., deterrence by delegitimization]. Whereas that strategy involves a tremendous amount of context that must be scrutinized throughout the government, this initiative could be less encumbered by those considerations."[75] In October 2020, the CNMF also began to use graphical images on Twitter in combination with its promotion of new adversarial malware samples uploaded on Virus Total to goad the Russians. One unnamed US official explained to CyberScoop, "We don't want something they can put on T-shirt. We want something that's in a PowerPoint their boss sees and he loses his s--- on them."[76] Whether those goading attempts have been fruitful is currently anyone's best guess.

In theory, burning adversarial tooling should create immense reputational and psychological effects on an adversarial team given that infrastructure and tooling must be (partially) abandoned, modified, or entirely redeveloped. However, the story of Iranian APT actor Oilrig (APT 34)—whose tooling, source code, and victim list were leaked on Telegram and GitHub between March and June 2019 in what was perhaps a CIA operation (conducted under the cover of a group calling itself Lab Dookhtegan)—should be a warning on blowback in practice.[77] Not only did Oilrig partially reuse some of its old tooling to stay alive, but it has churned out a host of entirely new malware products since July 2019.[78] In May 2020 for example, Oilrig became the first publicly known threat actor to incorporate the DNS-over-HTTPS protocol into its arsenal.[79] By July 2020, it revised its RDAT backdoor malware with a novel command-and-control channel that uses steganography to hide commands and data in bitmap images attached to emails.[80] One could assess that burning down Oilrig made life hellish for the Iranian team in the short term (i.e., inflicted severe reputational losses and substantially increased workload), but the team was also forced to innovate and reinvent itself in the long run (i.e.,

continuous reputational recovery and organizational restructuring). Similar to the logic of taking down botnets, burning down APT infrastructure and tooling rarely creates a lasting impact if operators are not caught and arrested.[81] Yet even in the botnet realm, adversarial attention and the psychological effects of having your infrastructure burned down can in some rare cases move operators to close down their botnets voluntarily.[82]

There are questions that remain unresolved in this context. How do we push adversarial operators to the psychological threshold that makes them give up or reinforces carelessness and disillusionment, in turn increasing adversarial mistakes? What concerns of adversaries define their psychological threshold? Can we somehow identify the elements of that threshold and where it might be situated for various threat actors and individual operators? And can we create cascading effects to hit multiple teams in the same country/organizational structure? These questions largely run along the bleeding edge linking cyberspace and the information warfare domain—connecting back to Der Derian's definition of *cyber deterrence* as being a part of psychological warfare.

Cross-Domain Deterrence

Cross-domain deterrence describes the spectrum of strategic measures a nation-state is willing to leverage outside the cyber domain in reaction to an event inside cyberspace. Actions can range from criminal indictments of cyber operatives and trolling campaigns in the information warfare space to imposing economic sanctions and launching retaliatory nuclear strikes.[83]

The primary problem with cross-domain deterrence is ascertaining whether such measures will deter future aggression in cyberspace or result in spillover effects that remove long-standing deterrence mechanisms elsewhere. Spearheaded by the US Department Justice (DOJ), the indictment of nation-state cyber operatives for crimes committed against US-based entities has become the focal point to hold individuals personally liable for their actions and orders followed. Some analysts claim this is evidence of a concerted naming and shaming strategy by the US government (i.e., deterrence by delegitimization). However, the DOJ's overarching legal aim is, and has always been, to attribute attacks and hold individuals accountable in a US court—whether adversarial cyber operators that hit non-military targets or foreign civilians that hit US entities. Tonya Ugoretz, deputy assistant director of the FBI's Cyber Division, aptly states, "nothing says attribution like an indictment."[84]

While nation-state cyber operatives indicted by the DOJ have remained outside the reach of US law enforcement, two cases stand out for counter-intelligence purpose. Although not per se a "cyber" operative, the case of Yanjun

Xu, deputy division director at the Chinese Ministry of State Security's Sixth Bureau in Jiangsu Province, highlights that the DOJ's indictments of foreign government operatives can net results abroad. Arrested in Brussels, Belgium, on April 1, 2018, Xu was extradited to the United States on October 9th.[85] According to US officials, Xu's extradition marked the first time a Chinese spy has been brought to the US to face prosecution.[86] On November 5, 2021, a federal jury convicted Xu of "conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies."[87] He is currently awaiting sentencing. The second case concerns Vladislav Klyushin, a Russian businessman and first deputy director of cybersecurity company M-13. Klyushin was arrested in Switzerland on March 21, 2021, on the request of US authorities who charged him with "alleged involvement in a global scheme to trade on non-public information stolen from U.S. computer networks that netted tens of millions of dollars in illegal profits."[88] While waiting for his extradition hearing, Swiss news outlet 24heures reported that former GRU (Russian intelligence agency) operative Ivan Sergeyevich Yermakov—wanted by the FBI for hacking into the DNC and interfering in the 2016 US presidential election—was actually employed by M-13.[89] Following Klyushin's extradition to the United States in December 2021, CNN reported in January 2020 that according to former US officials, Klyushin "could be a valuable asset in US efforts to gather more information on Russian interference in the 2016 election as well as other intelligence operations."[90] Similarly, Assistant US Attorney Seth B. Kosto argued at Klyushin's pretrial hearing in Boston that "we do submit that he's not simply any Russian citizen. . . . He is a Russian citizen who is employing a former military intelligence officer, who has a photograph in his internet service provider records of a medal of honor from the president of the Russian Federation."[91]

The US Treasury Department by contrast has been leveraging targeted economic sanctions since April 2015, when President Obama signed Executive Order 13694 and declared a national emergency to deal with the "increasing prevalence and severity of malicious cyber-enabled activities originating from . . . outside the United States [that] constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[92] In December 2016, EO13757 amended EO13694 "to include an Annex of sanctioned persons and to expand the scope of cyber-enabled activities subject to sanctions."[93] Other cyber-related sanction programs followed in subsequent years, including EO13722, Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea (March 2016) and the Countering America's Adversaries Through Sanctions Act (August 2017). Since then, the

Office of Foreign Assets Control (OFAC) has imposed cyber-related sanctions on close to 200 individuals and companies hailing from China, Iran, North Korea, and Russia.[94] Thus far, none of the countries in question have discernably decreased their cyber-related activities vis-à-vis the United States.

The European Union has partially emulated the US approach with EU Council Decision 2019/797 and Regulation 2019/796 of May 2019 on "restrictive measures against cyber-attacks threatening the Union or its Member States."[95] As of this writing, the council has imposed two cyber sanction packages that imposed asset freezes and travel restrictions on those listed. The first package on June 30, 2020, listed six individuals and two entities for the OPCW hack, WannaCry, NotPetya, and APT10's CloudHopper campaign.[96] The second package was imposed on October 22, 2020, against two GRU officers and the GRU's Unit 26165 for the 2015 Bundestag hack.[97] Similar to the sanctions imposed by the US Treasury Department, it is currently entirely unclear what kind, if any, effects EU cyber sanctions produce on the adversarial end. In contrast to US sanctions, EU restrictive measures do not serve as a vehicle for public attribution, as the decision to attribute or not remains a sovereign political decision of the individual EU member states. As of this writing, the EU nonetheless continues to argue in document after document that sanctions are "intended to prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace."[98] Probably most insightful when it comes to deterrence in this context is the UK's *National Cyber Strategy 2022*. It acknowledged for the first time that "the development of the autonomous UK cyber sanctions regime has added another disruptive tool that we have used to respond to incidents such as the WannaCry and NotPetya attacks. However, despite all this, our approach to cyber deterrence does not yet seem to have fundamentally altered the risk calculus for attackers."[99]

While it is indeed tempting to cross-connect preexisting deterrence frameworks elsewhere to the cyber domain, it is highly questionable whether the outcome is a more robust deterrence posture in cyberspace or a weakening of the deterrence posture in real space. For example, connecting nuclear deterrence to the cyber domain is probably an area where it could in fact be destabilizing or counterproductive. In January 2018, the *New York Times* reported that the language used in a draft of the 2018 *US Nuclear Posture Review* would "permit the use of nuclear weapons to respond to a wide range of devastating but non-nuclear attacks on American infrastructure, including what current and former government officials described as the most crippling kind of cyberattacks."[100] Amy Zegart, senior fellow at the Hoover Institution, questioned at the time, "Do we really think the United States government would launch a nuclear retaliatory strike after a cyberattack of how ever consequential

damage might be on the United States? . . . Lots of debate about that. Is that really a robust deterrence strategy? Probably not."[101]

Similarly, Harknett and Fischerkeller argued in 2017 that expanding deterrence to "include threats of law enforcement penalties, sanctions, and 'name and shame' approaches—denoted as whole-of-government deterrence—should be recognized for what it is—the addition of weaker forms of punishment because robust costs cannot be credibly imposed. Adding to a menu of weak options does not make deterrence stronger; it only reveals its inherent incompatibility with the challenge of the [cyber] domain."[102]

Having critically dismantled six deterrence mechanisms that have emerged over the past years, let us now turn to the questions of when cyber deterrence is deemed theoretically successful and when it is not.

When Is Cyber Deterrence Successful?

Testifying before the House Committee on Armed Services in 2017, RAND's Martin Libicki carefully explained that a successful deterrence posture in cyberspace necessitates four prerequisites: (1) the ability to correctly attribute cyberattacks, (2) the ability to effectively communicate US redlines, (3) the credibility of response if those red lines are crossed, and (4) the capabilities to successfully retaliate.[103]

To put Libicki's theory into practice, let us consider a few simple deterrence scenarios between a fictional country A (the aggressor) and a fictional country B (the defender). B's aim is to deter A's hostile behavior in cyberspace.

First, deterrence in cyberspace succeeds if country A abstains from initiating hostilities against country B. A's behavior could be due to a strategic rationale to avoid conflict, the negative outcome of a comprehensive cost-benefit analysis, B's ability to effectively communicate redlines, or none of the above. Lacking any evidence that might explain A's inaction, it is impossible to ascertain whether B's deterrence posture worked as desired. As such, none or all of Libicki's prerequisites would need to be fulfilled for this outcome to occur. This scenario has unfolded over the years with several researchers asserting that the absence of cyberattacks that cross the threshold to an armed attack is evidence of constraint and the functioning of deterrence in cyberspace.[104] While, logically, the absence of evidence can be considered evidence in itself, the absence of any theoretical underpinnings that can explain the supposed causal deterrence mechanisms at work creates a circular logic that delivers no answers at all.

Second, deterrence in cyberspace succeeds if country B responds (proportionally or disproportionally) to an attack from country A (within a proxi-

mate temporal range), and hostilities subsequently terminate. Three of Libicki's prerequisites would need to be fulfilled for this deterrence scenario to commence. The ability of effectively communicating redlines is redundant after the fact. However, we have not witnessed any exchange that would fit into this tit-for-tat category. This absence might indicate that escalation dynamics work entirely different in cyberspace—if at all—or might feed into a different political threat perception and strategic calculus that currently does not yet naturally translate down to the operational end and kicking off an immediate offensive response in cyberspace. Time likely moves magnitudes slower when it comes to decision-making processes for actions and reactions in cyberspace. Thus, decisions in real space and dynamics in cyberspace move independently from each other—in turn breaking down any escalation ladder before it can manifest itself. This time lag or causal disconnect would also explain why persistent engagement might not elicit an escalatory response or probably will not become entangled in an escalation ladder.[105]

Third, deterrence succeeds if country B responds out of domain to a cyberattack from country A by leveraging existing deterrence frameworks elsewhere (i.e., cross-domain deterrence), and subsequent adversarial actions in cyberspace terminate. All four of Libicki's prerequisites would need to be fulfilled for this scenario to occur. However, if, for instance, country B responds with economic sanctions or criminal indictments—which are not connected to traditional deterrence dynamics—then country A might not be deterred by B's retaliatory actions. The European Union and US Justice and Treasury Departments are currently locked into the latter scenario. It is uncertain whether their actions deter anyone or impose relevant costs on adversarial operations.

Fourth, cyber deterrence partially succeeds if country A attacks country B, and B responds by attacking country C due to misattribution. If country A deliberately left behind forensic evidence that would point toward country C (i.e., a false flag operation), then B's cyber deterrence posture inherently failed. However, if country B experienced a massive intelligence failure on its end and struck country C purely by mistake, then B's willingness to forcefully respond against country C might deter A from future attacks. In this scenario, only three of Libicki's prerequisites would need to be fulfilled. Given the complexity of this scenario, we have not yet witnessed anything like it in cyberspace.

Fifth, if hostilities between country A and B (1) can be curtailed to episodic engagements, (2) are limited in their intensity, (3) remain constrained to the cyber domain, and (4) do not pull in civilian targets or allied forces, cyber deterrence could theoretically succeed in what Herman Kahn describes as a state of limited conflict or "agreed battle."[106] However, if any of those tacitly

agreed on limitations are broken, deterrence fails, and escalation might reign supreme. For this interaction to play out, the only prerequisite necessary is for A and B to be able to correctly attribute each other's cyberattacks.

Scenario two combined with scenario five is where persistent engagement currently falls within the deterrence conundrum. Persistent engagement necessitates effectively communicating redlines (scenario two), but in contrast to traditional deterrence thinking, it also actively seeks out adversarial contact (scenario five).

When Is Cyber Deterrence Unsuccessful?

First, deterrence fails if country A conducts a "first strike" against country B without country B responding in self-defense. This reaction may be due to simple self-restraint, entanglement, or paralysis by analysis. A war-gaming example for such behavior was observed by Jacquelin Schneider, assistant professor in the Strategic and Operational Research Department at the US Naval College, during the DoD's annual war-game series Deterrence and Escalation Game in Review (DEGRE) in 2011. According to Schneider, the red team conducted offensive cyber operations against blue prior to any conventional military exchange. Instead of responding in kind, the blue defense lead explained, "I do not feel any of the cyber-attacks raised to the level where retaliation was needed and/or warranted! It was not risking nuclear war!"[107] Most of the other blue players echoed the sentiment, with one commenting that "cyber-attacks[,] although annoying[,] do not appear crippling."[108] Yet when blue discussed employing offensive cyber operations themselves, they immediately self-restrained by creating "an equivalency between cyber operations and nuclear attack," arguing that "any cyber attack would necessarily lead to a nuclear response."[109] The example illustrates the meatspace logics and assumptions being made on the strategic level when it comes to deterrence by punishment and cross-domain deterrence. They also fundamentally contradict the logics of war entailing the maximization versus the moderation of force. As Clausewitz wrote in *On War*, "to introduce the principle of moderation into the theory of war itself would always lead to logical absurdity."[110]

Second, cyber deterrence fails if country B preemptively attacks country A. Such was the case in DEGRE's 2012 exercise. As Schneider noted, the blue team went all in on preemptive cyber network operations to "degrade the enemy's ability to conventionally respond to US operations."[111] Schneider stated that "the perception by the blue team was that blue was just as vulnerable . . . as the red team [if not more so] . . . and therefore had to preemptively strike red's ability to conduct both cyber and kinetic attacks against blue com-

mand and control."[112] While this example is close to the logics of persistent engagement, it is also much more aggressive in nature. The caveat here is that while persistent engagement aims to create friction within an adversary's cyber capabilities and infrastructure, the blue team in DEGRE conducted offensive cyber operations to degrade and affect the red team's conventional war-fighting capabilities. That being said, country B might succeed in establishing a cyber deterrence posture after hostilities have ceased in this scenario.

Third, cyber deterrence fails when strategic signaling between both countries collapses at the most basic level. This was the case in DEGRE's 2013 wargame exercise. As Schneider explains, the blue team started by implementing strict rules of engagement on computer network exploitation to create a deterrence policy that would disincentivize red from conducting preemptive cyberattacks. This approach led to the rather absurd situation where blue worried about the detection of their cyber espionage efforts (not attack) amid a naval blockade that saw the exchange of gunfire and 20 of red's aircraft being shot down. Blue even tried to refine its deterrence policy by using cyber operations as a means of "signal[ing] potential capability while trying to avoid inadvertently signaling aggression or the willingness to escalate."[113] Schneider observes that "the red team failed to understand this elegant distinction."[114] In terms of responses, the blue team viewed red's cyberattacks "as less escalatory than other kinetic options and therefore believed it was not worth a response."[115]

And fourth, cyber deterrence fails if country A initiates hostilities, country B responds proportionally, and country A repeatedly escalates, potentially locking both into an escalation ladder. An example of such a crisis escalation scenario was on display during the four-day Schriever Wargame in 2010, hosted by Air Force Space Command and featuring some 600 military, civilian, and allied players.[116] According to Maj Gen Susan J. Helms, director of Plans and Policy at US Strategic Command, hostilities commenced when "in a response to a perceived provocation, a regional adversary disabled the cyber and space assets of a key US ally."[117] While debating how to deter attacks on US and allied space and cyber capabilities, the blue team realized that the enemy continued to attack time and time again and "was not deterred from further escalation." General Helms added, "As we came to learn, the leaders of this provocative regional state had defined their objectives (although those objectives were not obvious to us) and had already thought through the overall costs and benefits of their plan. In other words, they had assessed our likely behavior in the context of the scenario at hand, determined that, for them, the benefits of action outweighed the risks and they made their decision to 'move out.' At that point, options for deterrence by the US and her allies were 'late to need.' "[118]

Granted, these war-gaming examples are not ideal cases to adequately reflect the decision-making dynamics playing out regarding cyberspace. But they provide valuable insights into the flawed logics and strategic concerns that hinder developing sensible deterrence strategies and enabling operational tactics in the cyber domain.

Further Thoughts

In the absence of specific operational insights, tactical thinking, and deterrence success stories, we can still roughly deduce what deterrence effects are currently attainable given the publicly visible mechanisms and their limitations. First, we can build up a cyber deterrence posture, but we cannot create enough psychological pressure to deter adversarial actions. Second, we can change adversarial behavior, but we cannot deter adversarial targeting. Third, we can burn adversarial tooling and infrastructure, but we cannot deter adversaries from regenerating capabilities. Fourth, we can partially halt individual adversarial operations in the short term, but we cannot deter adversarial campaigns over the long run.

If we pair these four attainable effects and limitations with the uncertainty about whether escalation dynamics between state actors in cyberspace can and do manifest themselves similarly to real space, then one way to theoretically enhance cyber deterrence is to significantly ramp up offensive cyber operations. Persistent engagement does that to a certain degree, but it likely necessitates an even more aggressive posture. It would have to put aside the law of armed conflict and target adversarial civilian critical infrastructure and the private lives of individual adversarial operators and their loved ones during peacetime. While this level of aggression will likely be deemed by many lawyers, policy makers, and academic researchers as unlawful, inhumane, and morally despicable, this approach will also highly likely succeed in breaking down the psychological barriers and tactical misconceptions on the strategic level that the DEGRE and Schriever war games laid bare. The fundamentals that underpin current cyber deterrence thinking have to radically change because we likely cannot prevent adversarial targeting and operations against our civilian critical infrastructure and government IT systems. But we have the ability to impose a high price for adversaries hitting those systems.

Another potential avenue for advancing the cyber deterrence discussion is to increase focus on the counterintelligence and psychological warfare elements. If, as some researchers rightfully argue, cyber is fundamentally an intelligence contest, then fighting on that battlefield will naturally have to encompass physically hunting down and assassinating individual adversarial

cyber operators.[119] Other clandestine operations could also, for instance, seek to mobilize cybercriminals and other non-state hackers in adversarial or third-country territory to undermine government infrastructure and services or run false flag operations against third states. However, doing so would require that the Department of Justice use its intelligence to turn cybercriminals rather than indict them and publicly calling them out, while the CIA would have to move resources to train, support, and direct opposition hackers and other antigovernment forces in-country or in third countries. One potential example of this dynamic currently at play might be the group calling itself Indra, which ran a series of campaigns against Syrian targets in 2019–20 and is now notoriously known for attacking Iran's railroad system in July 2021.[120] According to Indra's Twitter account, the group's mission is to "bring a stop to the horrors of [Iran's Quds Force] and its murderous proxies in the region!"[121] Itay Cohen, senior researcher at Checkpoint, explains that "it is very possible that Indra is a group of hackers, made up of opponents of the Iranian regime, acting from either inside or outside the country, that has managed to develop its own unique hacking tools and is using them very effectively."[122] It could also well be that Indra is a fictional group created as a cover story to run offensive cyber operations spearheaded by a foreign intelligence agency.

On the psychological warfare front, some researchers have argued for the increased usage of hack-and-leak operations to discredit political figures in adversarial states, undermine the image of an adversarial government agency, or polarize the domestic public discourse in a target country. While doing so is certainly achievable given the right material, propagation tools, and narrative, it is doubtful whether the psychological outcome will culminate in deterrence. To produce deterrence effects, we likely must generate substantial psychological pressure amounting to a distinct form of terror that does not rely on uncertainty or doubt. However, it would signal our aggressiveness and willingness to inflict continuous pain and substantial suffering on individual operators and adversaries for the slightest infraction. Actions could include anything from doxing, stalking, and spinning the rumor mill to vicious campaigns harassing operators and their loved ones for weeks, months, or even years after they quit their service for the state. Over time, the adversarial operator will pay the price with the slow breakdown of their own psyche, family bonds, relationship with the state, place in society, and any other meaningful connection they had in their life. The goal of this approach would be the total dismantling of the operators themselves and the evaporation of any normalcy in their lives. The military targeting rules of necessity, proportionality, distinction, and humanity would not apply to this sort of operation, and any attempts to create reference points concerning what is deemed acceptable

or unacceptable behavior in cyberspace will likely have to seize to exist. If deterrence is the goal, then norms and international law—as currently conceptualized to apply in cyberspace—are highly likely a hindrance for deterrence effects to manifest themselves.

Conclusion

The discourse on cyber deterrence is a melting pot of ideas, concepts, and experiments meant to continuously twist, bend, and refine our understanding, from the conflict dynamics playing out in cyberspace to the psychological deterrence effects taking root inside the human mind. At least, that is how it ought to be. With the exception of persistent engagement, cyber deterrence thinking has to a large degree treaded intellectual water due to the absence of access to operational data and insights into the tactical decision-making processes. As a means to circumvent this substantial gap, academics have turned to recycling and transposing known deterrence mechanisms onto the cyber domain to mirror known outcomes elsewhere. Overall, those efforts have had limited practical success or could even be considered counterproductive to the creation of a cyber deterrence theory. The war games mentioned hold some key evidence for why a focus on strategic deterrence thinking alone is inherently insufficient when trying to optimize decision-making processes for conflict in the cyber domain. Until academics and war-game participants understand the realities of how militaries defend, fight, and win in cyberspace, cyber discussions—and to a larger degree, escalation dynamics—will remain deductive, reductive, and superficial. Nonetheless, the field of cyber deterrence is not a dead end. But progress in the field necessitates that researchers understand what effects we are currently able to create, what effects we cannot yet create, and which ones we would have to create to deter adversaries in and through cyberspace. Only through access to military thinking on the art of cyber, continuous experimentation, expedient practical adaptation, and out-of-the-box thinking will academics and military tacticians be able to piece together the puzzle that binds tactical and operational actions to produce the deterrence effects that we so desperately crave to create in cyberspace.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Der Derian, "Cyber-Deterrence."
2. Der Derian.
3. Cunningham, "Q&A with Ray Tomlinson on Creeper 'Virus.' "
4. Note: This assessment stands in stark contrast to Erica Borghard and Shawn Lonergan's assertions that "cyber escalation has not occurred because cyber operations are poor tools of escalation." See Borghard and Lonergan, "Cyber Operations as Imperfect Tools of Escalation," 122–45.
5. Nuttall, "Kosovo – the Internet War"; and Stout, "Crisis in the Balkans."
6. Guerrero-Saade et al., "Penquin's Moonlit Maze."
7. Soesanto, *Evolution of US Defense Strategy in Cyberspace*.
8. Bejtlich, "Greg Rattray Invented the Term Advanced Persistent Threat."
9. Harknett and Goldman, "Search for Cyber Fundamentals."
10. Soesanto and Smeets, "Cyber Deterrence: The Past, Present, and Future," 389–403.
11. See also Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*.
12. On the impossibility of cyber war, see Rid, *Cyber War Will Not Take Place*. On the infeasibility of cyber deterrence, see Valeriano and Maness, *Cyber War versus Cyber Realities*.
13. Brantly, "Cyber Deterrence Problem."
14. Wasser et al., *Comprehensive Deterrence Forum*.
15. Jarvis, "Deterrence Theory Revisited," 301.
16. Jarvis, 292.
17. Lupovici, "Emerging Fourth Wave of Deterrence Theory," 707.
18. Knopf, "Fourth Wave in Deterrence Research," 1.
19. Prior, "Resilience: The 'Fifth Wave,' " 63–80.
20. Bebber, "No Such Thing as Cyber Deterrence"; Nye, "Deterrence in Cyberspace"; Pomerleau, "Such a Concept as 'Cyber Deterrence?' "; and Fischerkeller and Harknett, "Persistent Engagement."
21. Tor, " 'Cumulative Deterrence,' " 92–117. Note: Some overlaps naturally exist between operational level cyber deterrence theories, such as persistent engagement, and cumulative deterrence mechanisms that focus on the credibility of the military threat and the willingness to operate.
22. "UK Teens to Get Free Access to CyberLand Platform"; Cimpanu, "Dutch Police Post 'Friendly' Warnings"; and Europol, "World's Most Dangerous Malware EMOTET Disrupted."
23. Europol, *European Union Serious and Organised Crime Threat Assessment*, 14.
24. Williams, "Nakasone: Cold War-Style Deterrence."
25. Aspen Institute, "CyberCom Leader Speaks on Defending the Nation."

26. Note: This paper tackles only deterrence mechanism that have influenced US and European thinking on cyber deterrence. As such, it does not discuss Uri Tor's cumulative deterrence (Israel), Yuan Yi's thinking on preventive, restraining deterrence, and others.

27. Garside, "Digital Resilience."

28. Nye, "Deterrence and Dissuasion in Cyberspace," 56.

29. Note: In 2014 Ben Buchanan created a cyber deterrence mosaic that ranged from general to specific on the x-axis and least restrictive to absolute on the y-axis. While the mosaic makes sense, his analysis never explained why adversaries exhibit different characteristics in the first place, that is, why they are forced to operate within different cost-benefit calculations. See Buchanan, "Cyber Deterrence Isn't Mad; It's Mosaic," 130–40.

30. Willard, "Understanding the Co-Evolution of Cyber Defenses," 23.

31. Vaas, "Podcast: Why Securing Active Directory Is a Nightmare."

32. Lee, "Fireside Chat – Cyber Industry Review."

33. van der Meulen, *Investing in Cybersecurity*.

34. Libicki, *Crisis and Escalation in Cyberspace*, 162.

35. Sharwood, "UK Names Russia as Source of NotPetya"; "Reckless Campaign of Cyber Attacks," UK National Cyber Security Centre; and UK Government, "Global Scale of Chinese Cyber Campaign."

36. Palmer, "Naming and Shaming Nations."

37. Lyngaas, "Right Country, Wrong Group?"; and "Destruction of APT3," Intrusion Truth. Note: The success of Intrusion Truth probably applies to few APTs. To date, the parameters of this success are unknown (too few data points).

38. Schmitt, "Peacetime Cyber Responses," 246.

39. Schmitt, 248.

40. Garamone, "Selva Discusses Nature of Nuclear Deterrence."

41. Lin, "Escalation Dynamics and Conflict Termination," 68.

42. Harknett and Goldman, "Search for Cyber Fundamentals," 81–88.

43. Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy," 386, 388–89.

44. US Cyber Command, "Achieve and Maintain Cyberspace Superiority," 6.

45. Barnes, "Cyberoperation against Russia Aimed at Protecting Elections"; and Barnes, "Cyber Command Operation Took Down Russian Troll Farm."

46. Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet"; and Villadsen and Hammond, "Trickbot Rising."

47. Sebenius, "Pre-Election Cyber Operations."

48. Barnes and Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran"; Ali and Stewart, "U.S. Carried Out Secret Cyber Strike"; and Barnes, "U.S. Military Has Acted against Ransomware Groups."

49. Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy," 386, 388–89.

50. US Cyberspace Solarium Commission, Final Report, 24.

51. Lonergan and Montgomery, "Defend Forward as a Whole-of-Nation Effort"; Bate et al., "Defending Forward by Defending Norms"; and Fischerkeller, "Cyberspace Solarium Commission Report."

52. Borghard and Lonergan, "Deterrence by Denial in Cyberspace," 22.

53. Borghard and Lonergan, 22.

54. Borghard and Lonergan, 3.

55. Vavra, "Pentagon Tried to Take Down These Hackers"; Villadsen and Hammond, "Trickbot Rising"; and Wong, "Russian Agency Created Fake Leftwing News Outlet."

56. Nye, "Deterrence and Dissuasion in Cyberspace."

57. See Nye and Keohane, *Power and Interdependence*; and Copeland, "Economic Interdependence and War," 5–41.

58. Brantly, "Conceptualizing Cyber Deterrence by Entanglement."

59. Murphy, "Why Would the U.S. Spy on Its Allies?"; and Boffey, "British Spies 'Hacked into Belgian Telecoms Firm.' "

60. United States District Court Southern District of California, "United States of America v. Ding Xiaoyang [et al.]," 17.

61. The White House, "President Xi Jinping's State Visit"; and Olson, "China Bolsters Undersea Warfare Power."

62. Bing and Martina, "U.S. Accuses China."

63. Poulson, "Obama's Cyberspace Peace with China."

64. Sobczak, "World's Most Dangerous Malware."

65. Giles, "Triton Is the World's Most Murderous Malware."

66. FireEye Intelligence, "TRITON Attribution." Note: On October 23, 2020, the US Treasury Department sanctioned the Central Scientific Research Institute of Chemistry and Mechanics for its role in developing Triton. See US Department of the Treasury, "Treasury Sanctions Russian Government Research Institution."

67. Foy, "Russia-Saudi Arabia Rapprochement."

68. Newman, "Russia Linked to Disruptive Industrial Control Malware."

69. Vavra, "North Korean Hackers Caught Snooping."

70. Nan, "China-North Korea Treaty Still Important."

71. Schelling, *Arms and Influence*, 124.

72. Libicki, *It Takes More Than Offensive Capabilities*, 2.

73. Vavra, "Cyber Command's Latest Warning." Note: It is clear that posting adversarial malware samples creates effects (burning tooling). It is, however, unclear whether the resulting effects are what Cyber Command wants to create.

74. USCYBERCOM Cybersecurity Alert (@CNMF_CyberAlert), "#CNMF has posted new malware to @VirusTotal."

75. Cimpanu, "US Cyber Command starts uploading foreign APT malware to @VirusTotal."

76. Vavra, "Trolling Russian, Chinese Hackers."

77. Greenberg, "Mystery Agent Is Doxing Iran's Hackers"; Dorfman et al., "Trump Order Gives CIA More Powers to Launch Cyberattacks"; and Cimpanu, "New Iranian Hacking Tool."

78. Bromiley et al., "Hard Pass: Declining APT34's Invite."

79. Cimpanu, "Iranian Hacker Group."

80. Falcone, "OilRig Targets Middle Eastern Telecommunications."

81. Garnaeva, "Kelihos/Hlux Botnet Returns."

82. *Taking Down Botnets*, US Senate, 113th Cong., 2d sess. (2014), 4 (statement of Cheri F. McGuire).

83. Mallory, *New Challenges in Cross-Domain Deterrence*, 7.

84. Lyngaas, "SamSam Outbreak Led to FBI Restructuring."

85. US Department of Justice, "Chinese Intelligence Officer Charged."

86. Lucas, "U.S. Charges Alleged Chinese Government."

87. US Department of Justice, "Jury Convicts Chinese Intelligence Officer."

88. "Kremlin-Linked Businessman Held in Switzerland," Swissinfo.ch; and US Department of Justice, "Russian National Extradited."

89. Botti, "Le Russe arrêté en Valais" ["The Russian Arrested in Valais"].

90. Koltrowitz, "Swiss Extradite Kremlin-Linked Russian"; and Lyngaass, "Russian Businessman's Kremlin Ties"

91. Andersen, "Russian Man Charged in Boston."

92. The White House, "Executive Order – 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.' "

93. Department of the Treasury, *Cyber-Related Sanctions Program*, 3.

94. Soesanto, "Hammer in Search of a Nail."

95. "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States"; and "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States."

96. "Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States."

97. "Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States."

98. See EU Council, "Malicious Cyber-Attacks"; and EU Council, "Solidarity with the United States on the impact of the SolarWinds cyber operation."

99. HM Government, *National Cyber Strategy 2022*, 25.

100. Sanger and Broad, "Countering Devastating Cyberattacks with Nuclear Arms." Note: The UK's 2021 Integrated Defense Review notes that "we reserve the right to review [the assurance on the non-use, or non-threat to use, nuclear weapons against any non-nuclear weapon state party to the Treaty on the Non-Proliferation of Nuclear Weapons] if the future threat of weapons of mass destruction, such as chemical and biological capabilities, or emerging technologies that could have a comparable impact, makes it necessary." See HM Government, *Global Britain in a Competitive Age*, 77.

101. Pomerleau, "Is There Such a Concept as 'Cyber Deterrence?'"

102. Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy," 386, 388–89.

103. Libicki, *It Takes More Than Offensive Capabilities*, 1–2.

104. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*; and Atlantic Council, "Healey: Cyber Deterrence Is Working."

105. Borghard and Lonergan similarly posit that (1) retaliatory offensive cyber operations may not exist at the desired time, (2) even when they exist, their effects are uncertain and limited, (3) decision-makers are generally hesitant to employ retaliatory offensive cyber operations, and (4) responding to cyber incidents with kinetic instruments will only be chosen in rare circumstances. See Borghard and Lonergan, "Cyber Operations as Imperfect Tools of Escalation," 122.

106. Kahn, *On Escalation*.

107. Schneider, "Cyber and Crisis Escalation," 20.

108. Schneider, 20.

109. Schneider, 20.

110. Clausewitz, *On War*, 14.

111. Schneider, "Cyber and Crisis Escalation," 21.

112. Schneider, 22.

113. Schneider, 25.

114. Schneider, 25.

115. Schneider, 25.

116. Dudney, "Hard Lessons at the Schriever Wargame," 58.

117. Helms, "Schriever Wargame 2010," 12.

118. Helms, 12.

119. Rovner, "Cyber War as an Intelligence Contest."

120. "Indra – Hackers behind Recent Attacks on Iran," Checkpoint.

121. Indra (@Indra17857623,

122. Bergman, "Mysterious Hacker Group."

Abbreviations

APT	advanced persistent threat
CNMF	Cyber National Mission Force
CSS	Central Security Service
DDoS	distributed denial of service
DEGRE	Deterrence and Escalation Game in Review
DNC	Democratic National Convention
DOJ	Department of Justice
GGE	group of governmental experts
IRA	Internet Research Agency
IT	information technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OEWG	Open-Ended Working Group
OFAC	Office of Foreign Assets Control
OPCW	Organisation for the Prohibition of Chemical Weapons
OT	operational technology
SOCTA	Serious and Organised Crime Threat Assessment
USCC	US Cyber Command

Bibliography

Ali, Idrees, and Phil Stewart. "Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials." Reuters, October 16, 2019. https://www.reuters.com/.

Andersen, Travis. "Russian Man Charged in Boston in Global Hacking Scheme Not 'Simply Any Russian Citizen,' Prosecutor Says in Urging No Bail for Defendant." *Boston Globe*, December 22, 2021. https://www.bostonglobe.com/.

Aspen Institute. "CyberCom Leader Speaks on Defending the Nation." Aspen Security Forum 2021. Posted November 3, 2021. YouTube video, 30:13-30:26. https://youtu.be/d56zPH0q89k.

Atlantic Council. "Healey: Cyber Deterrence Is Working," July 30, 2014. https://www.atlanticcouncil.org/.

Barnes, Julien E. "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections." *New York Times*, February 26, 2019. https://www.nytimes.com/.

———. "U.S. Begins First Cyberoperation against Russia Aimed at Protecting Elections." *New York Times*, October 23, 2018. https://www.nytimes.com/.

———. "U.S. Military Has Acted Against Ransomware Groups, General Acknowledges." *New York Times*, December 5, 2021. https://www.nytimes.com/.

Barnes, Julian E., and Thomas Gibbons-Neff. "U.S. Carried Out Cyberattacks on Iran." *New York Times*, June 22, 2019. https://www.nytimes.com/.

Bate, Laura, Phoebe Benich, Val Cofield, Karrie Jefferson, Ainsley Katz, and Sang Lee. "Defending Forward by Defending Norms," *Lawfare* (blog), March 11, 2020. https://www.lawfareblog.com/.

Bebber, Robert. "There Is No Such Thing as Cyber Deterrence. Please Stop." *Cipher Brief*, April 1, 2018. https://www.thecipherbrief.com/.

Bejtlich, Richard. "Greg Rattray Invented the Term Advanced Persistent Threat." *TaoSecurity Blog*, October 10, 2020. https://taosecurity.blogspot.com/.

Bergman, Ronen. "Mysterious Hacker Group Suspected in July Cyberattack on Iranian Trains." *New York Times*, August 14, 2021. https://www.nytimes.com/.

Bing, Christopher, and Michael Martina. "U.S. Accuses China of Violating Bilateral Anti-hacking Deal." Reuters, November 8, 2018. https://www.reuters.com/.

Boffey, Daniel. "British Spies 'Hacked into Belgian Telecoms Firm on Ministers' Orders.'" *The Guardian*, September 21, 2018. https://www.theguardian.com/.

Borghard, Erica D., and Shawn W. Lonergan. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* 13, no. 3 (2019): 122–45. https://www.airuniversity.af.edu/.

Borghard, Erica D., and Shawn W. Lonergan. "Deterrence by Denial in Cyberspace." *Journal of Strategic Studies*. Published online August 3, 2021. https://doi.org/10.1080/01402390.2021.1944856.

Botti, Dominique. "Le Russe arrêté en Valais emploie un hacker russe recherché" ["The Russian Arrested in Valais Employs a Wanted Russian Hacker"]. 24heures, September 2, 2021. https://www.24heures.ch/.

Brantly, Aaron. "Conceptualizing Cyber Deterrence by Entanglement." *Cyber Governance Blog*. College of International Studies, University of Oklahoma, March 15, 2018. http://www.ou.edu/.

Brantly, Aaron F. "The Cyber Deterrence Problem." Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Publications, October 2018. https://ccdcoe.org/.

Bromiley, Matt, Noah Klapprodt, Nick Schroeder, and Jessica Rocchio. "Hard Pass: Declining APT34's Invite to Join Their Professional Network." FireEye, July 18, 2019. https://www.fireeye.com/.

Buchanan, Ben. "Cyber Deterrence Isn't Mad; It's Mosaic." *Georgetown Journal of International Affairs*, International Engagement on Cyber IV (2014): 130–40.

Cimpanu, Catalin. "Dutch Police Post 'Friendly' Warnings on Hacking Forums." ZDNet, February 17, 2020. https://www.zdnet.com/.

———. "Iranian Hacker Group Becomes First Known APT to Weaponize DNS-over-HTTPS (DoH)." ZDNet, August 4, 2020. https://www.zdnet.com/.

———. "New Iranian Hacking Tool Leaked on Telegram." ZDNet, June 3, 2019. https://www.zdnet.com/.

———."US Cyber Command Starts Uploading Foreign APT Malware to @VirusTotal." ZDNet, November 8, 2018. https://www.zdnet.com/

Clausewitz, Carl von. *On War*. Oxford World's Classics. Edited and translated by Michael Howard and Peter Paret. UK: Oxford University Press, 2008.

Conti, Gregory, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press, 2017.

Copeland, Dale. "Economic Interdependence and War: A Theory of Trade Expectations." *International Security* 20, no. 4 (1996): 5–41. https://doi.org/10.2307/2539041.

"Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." *Official Journal of the European Union*, L 129, May 17, 2019. https://eur-lex.europa.eu/.

"Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." *Official Journal of the European Union*, L 1127, July 30, 2020. https://eur-lex.europa.eu/.

"Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." *Official Journal of the European Union*, L 351 I, October 20, 2020. https://eur-lex.europa.eu/.

"Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States." *Official Journal of the European Union*, L 129 I, May 17, 2019. https://eur-lex.europa.eu/.

Cunningham, Jordan Spencer. "Q&A with Ray Tomlinson on Creeper 'Virus.'" nerdology.org, November 21, 2014. https://nerdology.org/.

Department of the Treasury. *Cyber-Related Sanctions Program*. Washington, DC: Dept. of the Treasury, Office of Foreign Assets Control, July 3, 2017. https://home.treasury.gov/.

Der Derian, James. "Cyber-Deterrence," *Wired*, September 1, 1994. https://www.wired.com/.

Dorfman, Zach, Kim Zetter, Jenna McLaughlin and Sean D. Naylor. "Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks." Yahoo News, July 15, 2020. https://news.yahoo.com/.

Dudney, Robert S. "Hard Lessons at the Schriever Wargame." *Air Force Magazine* 94, no. 2 (February 2011): 58–61. http://www.airforcemag.com/.

EU Council. "Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation." Press release, April 15, 2021. https://www.consilium.europa.eu/.

———. "Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack." Press release, October 22, 2020. https://www.consilium.europa.eu/.

Europol. *European Union Serious and Organised Crime Threat Assessment: A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime*. Luxembourg: Publications Office of the European Union, 2021. https://www.europol.europa.eu/.

———. "World's Most Dangerous Malware EMOTET Disrupted through Global Action." Europol, November 18, 2021. https://www.europol.europa.eu/.

Falcone, Robert. "OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory." Palo Alto Networks – Unit 42, July 22, 2020. https://unit42.paloaltonetworks.com/.

FireEye Intelligence. "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers." Mandiant, October 23, 2018. https://www.fireeye.com/.

Fischerkeller, Michael P. "The Cyberspace Solarium Commission Report and Persistent Engagement." *Lawfare* (blog), March 23, 2020. https://www.lawfareblog.com/.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (2017): 386, 381–93. https://doi.org/10.1016/j.orbis.2017.05.003.

———. "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation." Institute for Defense Analysis, May 2018. https://www.ida.org/.

Foy, Henry. "Russia-Saudi Arabia Rapprochement Reshapes More Than the Oil Market." *Financial Times*, October 29, 2018. https://www.ft.com/content/.

Garamone, Jim. "Selva Discusses Nature of Nuclear Deterrence at Mitchell Institute Forum." Joint Chiefs of Staff website, August 3, 2017. https://www.jcs.mil/.

Garnaeva, Maria. "Kelihos/Hlux Botnet Returns with New Techniques." *Securelist* (blog). Kaspersky, January 31, 2012. https://securelist.com/.

Garside, Debbie. "Digital Resilience – a Step up from Cybersecurity." CSO Online, August 1, 2018, https://www.csoonline.com/.

Giles, Martin. "Triton Is the World's Most Murderous Malware, and It's Spreading." *MIT Technology Review*, March 5, 2019. https://www.technologyreview.com/.

Glaser, Charles. *Deterrence of Cyber Attacks and U.S. National Security*. Cyber Security and Policy Research Institute Report GW-CSPRI-2011-5. Washington, DC: George Washington University, June 1, 2011. https://cspri.seas.gwu.edu/.

Greenberg, Andy. "A Mystery Agent Is Doxing Iran's Hackers and Dumping Their Code." *Wired,* April 18, 2019. https://www.wired.com/.

Guerrero-Saade, Juan Andres, Costin Raiu, Daniel Moore, and Thomas Rid. "Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage." Kaspersky Lab, March 2018. https://media.kasperskycontenthub.com/.

Harknett, Richard J., and Emily Goldman. "The Search for Cyber Fundamentals." *Journal of Information Warfare* 15, no. 2 (Spring 2016): 81–88, https://www.jinfowar.com/.

Helms, Susan J. "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain." *High Frontier* 7, no. 1 (November 2010): 12–15. https://www.afspc.af.mil/.

HM Government. *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*. UK: APS Group, March 2021. https://assets.publishing.service.gov.uk/.

———. *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK*. UK: National Archives, Her Majesty's Stationery Office, 2021. http://data.parliament.uk/.

Indra (@Indra17857623). Twitter, accessed February 1, 2022. https://twitter.com/Indra17857623.

"Indra–Hackers behind Recent Attacks on Iran." Checkpoint, August 14, 2021. https://research.checkpoint.com/.

Jarvis, Robert. "Deterrence Theory Revisited." *World Politics* 31, no. 2 (1979): 289–324. https://doi.org/10.2307/2009945.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. New York: Frederick A. Praeger, 1965.

"Kremlin-Linked Businessman Held in Switzerland." swissinfo.ch, June 9, 2021. https://www.swissinfo.ch/.

Knopf, Jeffrey W. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy* 31, no. 1 (2010): 1–33. https://doi.org/10.1080/13523261003640819.

Koltrowitz, Silke. "Swiss Extradite Kremlin-Linked Russian Businessman to United States." Reuters, December 20, 2021. https://www.reuters.com/.

Lee, Robert M., CEO Dragos. Global Cybersecurity Forum Virtual Dialogue. "Fireside Chat – Cyber Industry Review." Streamed live on April 7, 2021. YouTube video, 2:47:56-2:48:12. https://www.youtube.com/

Libicki, Martin C. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corporation, 2012. https://www.rand.org/.

———. *It Takes More Than Offensive Capabilities to Have an Effective Cyber-deterrence Posture*. CT-465. Testimony presented before the House Armed Services Committee. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/.

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. https://www.airuniversity.af.edu/.

Lonergan, Erica D., and Mark Montgomery. "Defend Forward as a Whole-of-Nation Effort." *Lawfare* (blog), March 11, 2020. https://www.lawfareblog.com/.

Lucas, Ryan. "U.S. Charges Alleged Chinese Government Spy with Stealing U.S. Trade Secrets." NPR, October 10, 2018. https://www.npr.org/.

Lupovici, Amir. "The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda." *International Studies Quarterly* 54, no. 3 (2010): 705–32. http://www.jstor.org/stable/40931133.

Lyngaas, Sean. "Right Country, Wrong Group? Researchers Say It Wasn't APT10 That Hacked Norwegian Software Firm." Cyberscoop, February 12, 2019. https://www.cyberscoop.com/.

———. "Russian Businessman's Kremlin Ties Could Prove Intelligence 'Gold Mine' for US, Former Official Says." CNN, January 3, 2022. https://edition.cnn.com/.

———. "SamSam Outbreak Led to FBI Restructuring, Top Official Says." CyberScoop, April 4, 2019. https://www.cyberscoop.com/.

Mallory, King. *New Challenges in Cross-Domain Deterrence*. Perspective Series. Santa Monica, CA: RAND Corporation, 2018). https://www.rand.org/.

Murphy, Christopher J. "Why Would the U.S. Spy on Its Allies? Because Everyone Does." CNN, June 25, 2015. https://edition.cnn.com/.

Nakashima, Ellen. "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election." *Washington Post*, October 9, 2020. https://www.washingtonpost.com/.

Nan, Li. "60 Years On, China-North Korea Treaty Still Important for Cooperation and Peace." NK News, July 10, 2021. https://www.nknews.org/.

Newman, Lily Hay. "Russia Linked to Disruptive Industrial Control Malware." *Wired*, October 23, 2018. https://www.wired.com/.

Nuttall, Chris. "Kosovo – the Internet War." BBC News, April 16, 1999. http://news.bbc.co.uk/.

Nye, Joseph S., Jr. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (Winter 2016/17): 44–71. https://doi.org/10.1162/ISEC_a_00266.

———. "Deterrence in Cyberspace." Project Syndicate, June 3, 2019. https://www.project-syndicate.org/.

Nye, Joseph S., Jr., and Robert Keohane. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown & Co. 1977.

Olson, Wyatt. "China Bolsters Undersea Warfare Power through Stolen US Technology, Admiral Says," *Stars and Stripes*, April 18, 2018. https://www.stripes.com/.

Palmer, Danny. "Naming and Shaming Nations That Launch Cyberattacks Does Work, Say Intel Chiefs." ZDNet, April 26, 2019. https://www.zdnet.com/.

Pomerleau, Mark. "Is There Such a Concept as 'Cyber Deterrence'?" Fifth Domain, April 30, 2019. https://www.fifthdomain.com/.

Poulson, Kevin. "Obama's Cyberspace Peace with China Is Just About Dead." *Daily Beast*, December 20, 2018. https://www.thedailybeast.com/.

Prior, Tim. "Resilience: The 'Fifth Wave' in the Evolution of Deterrence." In *Strategic Trends 2018: Key Developments in Global Affairs*, edited by Oliver Thränert and Martin Zapf, 63–80. Zürich: Center for Security Studies, ETH Zürich, 2018. https://css.ethz.ch/.

"Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed." UK National Cyber Security Centre, October 3, 2018. https://www.ncsc.gov.uk/.

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2012.

Rovner, Joshua. "Cyber War as an Intelligence Contest." War on the Rocks, September 16, 2019. https://warontherocks.com/.

Sanger, David E., and William J. Broad. "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms." *New York Times*, January 16, 2018. https://www.nytimes.com/.

Schelling, Thomas. *Arms and Influence*. New Haven, CT: Yale University Press 1966.

Schmitt, Michael N. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum." *Harvard National Security Journal* 8, no. 2 (2017): 239–82. https://harvardnsj.org/.

Schneider, Jacquelyn. "Cyber and Crisis Escalation: Insights from Wargaming." Newport, RI: US Naval War College, 2017. https://paxsims.files.wordpress.com/.

Sebenius, Alyza. "U.S. Conducted More Than Two Dozen Pre-Election Cyber Operations." Bloomberg, March 25, 2021. https://www.bloomberg.com/.

Sharwood, Simon. "UK Names Russia as Source of NotPetya, USA Follows Suit." The Register, February 15, 2018. https://www.theregister.co.uk/.

Sobczak, Blake. "The Inside Story of the World's Most Dangerous Malware." E&E News, March 7, 2019. https://www.eenews.net/.

Soesanto, Stefan. "A Hammer in Search of a Nail: EU Sanctions and the Cyber Domain." *Journal of International Affairs*, December 6, 2018. https://jia.sipa.columbia.edu/.

———. Trend Analysis: The Evolution of US Defense Strategy in Cyberspace (1988–2019). Zürich: Center for Strategic Studies, ETH Zürich, August 2019. https://css.ethz.ch/.

Soesanto, Stefan, and Max Smeets. "Cyber Deterrence: The Past, Present, and Future." In *NL ARMS Netherlands Annual Review of Military Studies 2020* edited by Frans Osinga and Tim Sweijs, 385–40. The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_20.

Stout, David. "Crisis in the Balkans: China Protests Crash White House Web Site." *New York Times*, May 12, 1999. https://www.nytimes.com/.

Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Network, Hearing before the US Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism. US Senate, 113th Cong., 2d sess. (2014). (Statement of Cheri F. McGuire, Vice President, Global Government Affairs and Cybersecurity Policy, Symantec Corporation.) https://www.judiciary.senate.gov/.

"The Destruction of APT3." Intrusion Truth, May 22, 2018. https://intrusiontruth.wordpress.com/.

The White House. "Executive Order – 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,' " April 1, 2015. https://obamawhitehouse.archives.gov/.

———. "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015. https://obamawhitehouse.archives.gov/.

Tor, Uri. " 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40, nos. 1–2 (2017): 92–117. https://doi.org/10.1080/01402390.2015.1115975.

UK Government. "UK and Allies Reveal Global Scale of Chinese Cyber Campaign." Press release, December 20, 2018. https://www.gov.uk/.

"UK Teens to Get Free Access to CyberLand Platform to Improve Cyber Skills." *Government Computing*, May 8, 2020. https://www.governmentcomputing.com/.

United States District Court Southern District of California. "United States of America v. Ding Xiaoyang, Cheng Qingmin, Zhu Yunmin, and Wu Shurong," May 28, 2021. https://www.justice.gov/.

USCYBERCOM Cybersecurity Alert (@CNMF_CyberAlert). "#CNMF has posted new malware to @VirusTotal." Twitter, November 5, 2018, 1:10 p.m. https://twitter.com/.

US Cyber Command. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command." Released March 23, 2018. https://www.cybercom.mil/.

US Cyberspace Solarium Commission. Final Report, March 2020. https://drive.google.com/.
US Department of Justice. "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies," October 10, 2018. https://www.justice.gov/.
———. "Jury Convicts Chinese Intelligence Officer of Espionage Crimes, Attempting to Steal Trade Secrets," November 5, 2021. https://www.justice.gov/.
US Department of Justice, US Attorney's Office, District of Massachusetts. "Russian National Extradited for Role in Hacking and Illegal Trading Scheme," December 20, 2021. https://www.justice.gov/.
US Department of the Treasury. "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware." Press release, October 23, 2020. https://home.treasury.gov/.
Vaas, Lisa. "Podcast: Why Securing Active Directory Is a Nightmare." Threatpost, July 28, 2021. https://threatpost.com/.
Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press, 2015.
van der Meulen, Nicole. *Investing in Cybersecurity*. RR-1202. Cambridge, UK: RAND Europe, WODC, 2015. https://repository.wodc.nl/.
Vavra, Shannon. "How the Pentagon Is Trolling Russian, Chinese Hackers with Cartoons." CyberScoop, November 12, 2020. https://www.cyberscoop.com/.
———. "North Korean Hackers Caught Snooping on China's Cyber Squad." *Daily Beast*, November 22, 2021. https://www.thedailybeast.com/.
———. "The Pentagon Tried to Take Down These Hackers. They're Back." *Daily Beast*, July 12, 2021. https://www.thedailybeast.com/.
———. "Why Cyber Command's Latest Warning Is a Win for the Government's Information Sharing Efforts." CyberScoop, July 10, 2019. https://www.cyberscoop.com/.
Villadsen, Ole, and Charlotte Hammond. "Trickbot Rising – Gang Doubles Down on Infection Efforts to Amass Network Footholds." *Security Intelligence*, October 13, 2021. https://securityintelligence.com/.
Wasser, Becca, Ben Connable, Anthony Atler, and James Sladden, eds. *Comprehensive Deterrence Forum – Proceedings and Commissioned Papers*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/.
Willard, Gerald N. "Understanding the Co-Evolution of Cyber Defenses and Attacks to Achieve Enhanced Cybersecurity." *Journal of Information Warfare* 14, no. 2 (April 2015): 17–31. https://cryptome.org/.

Williams, Brad D. "Nakasone: Cold War-Style Deterrence 'Does Not Comport to Cyberspace.' " Breaking Defense, November 4, 2021. https://breakingdefense.com/.

Wong, Julie Carrie. "Russian Agency Created Fake Leftwing News Outlet with Fictional Editors, Facebook Says." *The Guardian*, September 1, 2020. https://www.theguardian.com/.