REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/08/2021	Master of Military Studies Research Paper	August 2020 - April 2021

4. TITLE AND SUBTITLE
Persistent Engagement and Defend Forward: the United States' Critical Role in Cyberspace

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Seagroatt, Sarah B., Major, US Army

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
Persistent Engagement (PE), and its sister framework, Defend Forward (DF), are critical elements of the 2018 Department of Defense (DoD) Cyber Strategy. These frameworks drastically shift the United States' strategic approach to cyberspace, marking the departure from a passive and reactive approach to proactive forward engagement. Since the DoD unveiled its 2018 Cyber Strategy, scholars have debated the merits and pitfalls of these frameworks. This paper will argue that the United States must continue to implement PE and DF for military, economic, and strategic reasons.

15. SUBJECT TERMS
cyber; defend forward; persistent engagement; strategy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University/Command and Staff
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	25	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

PERSISTENT ENGAGEMENT AND DEFEND FORWARD: THE UNITED STATES' CRITICAL ROLE IN CYBERSPACE

AUTHOR:

MAJOR SARAH BETH SEAGROATT

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member: Dr. Jill Goldenziel
Approved: _____
Date: 4/8/2021

MMS Mentor Team and Oral Defense Committee Member: Dr. Jorge Benitez
Approved: _____
Date: 4/8/21

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

PERSISTENT ENGAGEMENT AND DEFEND FORWARD: THE UNITED STATES' CRITICAL ROLE IN CYBERSPACE

AUTHOR:

MAJOR SARAH BETH SEAGROATT

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member: Dr. Jill Goldenziel
Approved: _____
Date: _____

MMS Mentor Team and Oral Defense Committee Member: Dr. Jorge Benitez
Approved: _____
Date: _____

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Illustrations

Page

Table of Contents

Executive Summary

Title: Persistent Engagement and Defend Forward: The United States' Critical Role in Cyberspace

Author: Major Sarah Beth Seagroatt, United States Army

Thesis: This paper will argue that the United States should continue to implement Persistent Engagement and Defend Forward in support of a national cyber strategy. While these elements of the current cyber strategy incur risks, the U.S. must continue to incorporate them for military, economic, and strategic reasons.

Discussion: Persistent Engagement (PE), and its sister framework, Defend Forward (DF), are critical elements of the 2018 Department of Defense (DoD) Cyber Strategy. These frameworks drastically shift the United States' strategic approach to cyberspace, marking the departure from a passive and reactive approach to proactive forward engagement. Since the DoD unveiled its 2018 Cyber Strategy, scholars have debated the merits and pitfalls of these frameworks. This paper will argue that the United States must continue to implement PE and DF for military, economic, and strategic reasons.

This paper will begin by introducing the primary arguments related to PE and DF. It will define critical terms, examine pertinent events in U.S. cyber strategy evolution, and highlight significant literature germane to this topic. This paper will then argue that the United States should continue implementing PE and DF for military, economic, and strategic reasons. Militarily, this paper will explain that these frameworks support the National Security Strategy (NSS), National Defense Strategy (NDS), and the National Military Strategy (NMS) by enabling proactive cyber operations capable of defense, denial, degradation, disruption, and defeat. It will explain how PE and DF fit into military deterrence theory as outlined by the Joint Chiefs of Staff. It will also lay out recent critical shifts in cyberspace planning which support PE and DF. Economically, this paper will argue that the United States must maintain these frameworks because the monetary costs to the U.S. government and American companies of failing to do so are too egregious. It will describe three primary ways cyberattacks cause damage: Intellectual Property (IP) theft, costs to American companies, and long-term erosion of trust in the federal system. Finally, this paper will discuss the strategic benefits of the PE and DF frameworks. It will argue that creating norms through tacit bargaining will be more effective than the explicit bargaining primarily used in U.S. cyber strategies prior to 2018. It will examine the strategic potential of international litigation to develop cyber norms. This paper will conclude by recommending that the United States continue to implement PE and DF in future cyber efforts.

Conclusion: Future U.S. cyber strategies should continue to incorporate the Defend Forward and Persistent Engagement frameworks because they represent the best military, economic, and strategic option for U.S. cyber efforts.

Acknowledgments

I would like to thank God, TH, and MH. Also, my mentors for their flexibility and understanding.

Introduction

Two years ago, the United States put forward a pivotal document titled the 2018 Department of Defense (DoD) Cyber Strategy. This document drastically shifted the United States' approach to cyber strategy, marking the departure from a passive, defensive cyber strategy to a more proactive and offensive one. The interdependent frameworks of Persistent Engagement (PE) and Defend Forward (DF) are two critical elements of this new strategy. Scholars, politicians, and military leaders have debated the 2018 Cyber Strategy with increasing fervor over the last two years. Due to the uniqueness of cyberspace and the implications of this strategic shift, much has been written in support of and against this strategy.

PE and DF are mutually integrated frameworks guiding U.S. operations in cyberspace. PE encompasses the continuously active and reactive cyber operations which capitalize on the partner-enabled forward cyber presence of DF. As General Nakasone (Commander of the United States Cyber Command (USCC), Director of the National Security Agency, and Chief of the Central Security Service) explained in a statement before the House Committee on Armed Services last year, DF is the cornerstone of DoD cyber strategy, and "drives Cyber Command's doctrine called persistent engagement: [DF] enables partners with unique insights, and it stands ready to act by imposing costs when authorized."[1] Nakasone clarifies the intent of PE and DF in a *Joint Forces Quarterly* article, explaining that PE "will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace… and [over time] raise the costs that our adversaries incur from hacking the United States."[2] The reciprocally supportive PE and DF frameworks encompass various proactive, and even preemptive, operations in cyberspace. While most PE and DF's details remain classified, a general concept of these frameworks is sufficient to understand the significant shift they herald.

One of the most critical actions supporting PE and DF is the 2019 National Defense Authorization Act (NDAA) declaration that cyber operations are *traditional military activities*, or TMA. MG Charles Moore, former USCC Director of Operations, notes that without this designation, USCC would need to "declare or make very overt any of our operations and acknowledge that it's being done by the DoD and the USA -- not very conducive to being successful inside the cyber domain…by declaring it a traditional military activity it allowed us to move away from that."[3] Cyber operations as TMA enable the U.S. government to take immediate, continuous, clandestine actions against adversaries in the ever-evolving cyber domain.

Cyberspace is unique in a few ways. First, it is a nascent domain, and as such, cyber strategy is a relatively new field.[4] Cyber strategy is also distinctive because it is highly dynamic. Because of this, the publication date of the literature is essential to note. Furthermore, due to the highly classified nature of DoD actions and regulations in cyberspace, the publications available to the general public are only a snapshot of what resides in classified environments. Finally, because of the recent cybersecurity policy changes, official government documents, statements, and articles comprise a significant portion of the literature.

Defining the Cyber Landscape

A few definitions are necessary in order to understand this topic. Because this domain is new and burgeoning compared to other domains, the terminology is often misused. Also, civilian and government definitions are frequently contradictory. This paper will use the definitions put forth by the Cybersecurity and Infrastructure Agency (CISA), a federal agency within the U.S. Department of Homeland Security (DHS), and by the DoD Joint Chiefs of Staff. The first is

cyberspace, which is "the interdependent network of information technology infrastructures, that includes the internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] Another is *cybersecurity*, which is the "strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[6] Finally, *cyberspace operations*, also known as *cyber operations* or CO, are "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[7]

It is also important to understand the framework for U.S. cyber mission sets, which fall into three broad buckets: DoD Information Network (DODIN) Operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). The DODIN is the "global infrastructure carrying DoD, national security, and related intelligence community information and intelligence."[8] DODIN Operations are the front line of defense: they "design, build, configure, secure, and sustain DoD communications systems and networks across the entire DODIN."[9] DCO are intended "to defend DoD or other friendly cyberspace…these are both passive and active defense operations and are conducted inside and outside of DODIN."[10] OCO are "intended to project power by the application of force in and through cyberspace… these operations are authorized like operations in the physical domains."[11]

Finally, and most importantly, it is essential to understand the general idea and purpose of the PE and DF frameworks. As retired Army Colonel Gary Corn, former General Counsel at

USCC, explains, PE is the operational framework that encourages proactive over reactive efforts in cyberspace.[12] David Luber, former Executive Director of USCC and interim NSA Cybersecurity Director, explains this new strategy as, "persistent engagement with persistent force…no longer reactive, but actually operating in cyberspace in an area where there is no sanctuary or operational pause… we are in constant contact with our enemies."[13] If PE focuses on the "when," DF focuses on the "where." DF, best understood as "counter cyber operations," encapsulates the operational actions focused on attacking hostile aggressors as close to the source as possible.[14] By operating closer to the source of aggression, DF enables prompt defensive actions. DF's purpose, according to Corn, is "to proactively contest, disrupt and degrade cyber aggression at or as close as practicable to its source before it reaches U.S., allied and partner networks."[15] PE and DF are broad frameworks that emphasize continuous and quick operations in cyberspace.

Despite the significant amount of discussion devoted to PE and DF frameworks, confusion still arises. As Jacquelyn Schneider, a Senior Advisor to the Cyberspace Solarium Commission and prominent cyber scholar, notes: "There is still significant debate about the scope of the actions or effects defend forward might encompass, all the way from benign cyber network exploitation of adversary cyber capabilities, to cyber-enabled influence operations, to cyberattacks that degrade an adversary's ability to use its offensive cyber capabilities. What is clear, however, is that the Defense Department believes defend forward actions can be preemptive, which is possible only with persistent engagement."[16] A further misconception of the PE and DF frameworks is that their primary purpose is deterrence. While strategic deterrence is a long-term ancillary benefit of PE and DF, the primary purpose of PE and DF is to disrupt adversary behavior to enable tactical, operational, and strategic initiative.[17]

History of the U.S. Cyber Strategy

Before the 2018 Strategy, the U.S. government struggled to develop and implement a practical strategic approach to cybersecurity. In the last decade alone, the focus of U.S. cyber strategy has pivoted from reactive deterrence to proactive disruption. In 2011, President Obama put out the International Strategy for Cyberspace, which optimistically focused on creating norms through passive discourse and defensive deterrence. This strategy's subtitle – "prosperity, security, and openness in a networked world" – effectively summarizes its hopeful attitude.[18] This document was the international version of the 2011 Strategy for Operating in Cyberspace.[19] Unfortunately, this approach did not deter aggressors. The period between 2011 and 2015 saw a significant uptick in hostile cyber incidents.[20] During this time, existing U.S. cyber policies, strategies, and authorities significantly hamstrung the DoD's ability to react in a timely and efficient manner to cyberattacks.

Some of the attacks that occurred during the Obama Administration forever colored the cyber landscape from a U.S. perspective. One of the most impactful events was the Russian disruption of the 2016 U.S. elections, which became the primary driving force behind the shift in DoD cyber strategy. However, other attacks during this time also significantly affected U.S. strategy and policy, including the Chinese Office of Personnel Management (OPM) hack stealing unprecedented amounts of Personally Identifiable Information (PII) of federal workers and Intellectual Property (IP), the North Korean ransomware attacks against Sony, and Iran's attacks on Saudi Aramco with the virus now known as "Shamoon."[21]

Despite the widespread acknowledgment in 2015 that the Obama administration's cyber policies failed to curtail adversary actions, the U.S. did little about it except to double down on deterrence efforts. In 2015, the Secretary of Defense Ash Carter published a new DoD Cyber

Strategy. This document was essentially a more detailed version of the 2011 Strategy. However, it did elucidate significant workforce and structural changes to the DoD cyber force, including the creation of a new unified combatant command (USCC) and the development of the DoD's Cyber Mission Force. The 2015 Strategy did two other significant things: it discussed offensive operations, and it noted the importance of attribution in cyber operations.[22]

In 2018, DoD unveiled its pivotal cyber strategy. Congress supported many of the changes in the 2018 Strategy with monetary and authority realignments through National Defense Authorization Acts (NDAAs) in subsequent years. In 2019, Congress approved the creation of the Cyberspace Solarium Commission – a bipartisan and intergovernmental group focused on developing U.S. cyber strategy. The report published by the Solarium Commission is a central document in the shifting landscape of U.S. cyber strategies.[23] While this report uses the terminology of deterrence calling for a "layered cyber deterrence" strategy – the specific shifts that it recommends directly enable PE and DF frameworks.

For example, before 2018, approval for offensive cyber operations was lengthy, laborious, and prevented the national command authority (NCA) from delegating responsibility. Because of this, according to one U.S. senator speaking in an unclassified environment, the United States did not conduct even a single offensive operation in the five years between 2013 and 2018.[24] The Solarium Commission's report prioritizes streamlining the approval process and delegating approval authority for DoD operations in cyberspace. The focus on streamlining was not unprecedented: in 2018, the Trump administration published National Security Presidential Memorandum (NSPM) 13, superseding President Obama's Presidential Policy Directive (PPD) 20 and allowing for delegated authority from the President to the Secretary of Defense for

specific missions in cyberspace.[25] However, while NSPM streamlined some of the authorities, many remain confined in convoluted and archaic legal shackles.[26]

The DoD failures to deter cyberattacks spurred criticism from a handful of prominent voices. Two such critics were Michael Fischerkeller and Richard Harknett – prominent scholars with extensive experience within the DoD working on various cyber-focused staffs at the National Security Agency (NSA), the Joint Chiefs of Staff (JCS), and USCC. In 2017, they co-authored a piece for *Orbis* titled "Deterrence is Not a Credible Strategy for Cyberspace."[27] This article offered PE as the best means for shaping norms, arguing against the operational restraint put forth up until that point. Along with other prominent voices in the field, these two individuals laid the foundation for the innovative 2018 departure from deterrence to disruption.

The 2018 Strategy dramatically shifts the U.S. posture in cyberspace.[28] As Senator Mike Rounds, then chair of the Senate Committee on Armed Services (SASC), compared the situation to the quaint task of trapping mice in an interview with *Fifth Domain* magazine,

> Number one, you've got to be able to have mouse traps in the house. Second of all you've got to plug the holes where the mice are getting into the house … But it's also very important that you put offensively, that you put out bait on the outside and trap as many of those mice as possible before they ever get into the house… That's what this is all about. Tracing them down to where they're at and taking these mice and rats out before they can get into our house.[29]

While this analogy may seem quaint, it is one of the more apt descriptors of the new strategy's purpose and intent. In other words, as JD Work (a member of the U.S. Cyberspace Solarium Commission) explained in a recent interview, the purpose of PE and DF is to maintain the initiative.[30] This strategy has been widely misunderstood, according to COL (ret) Gary Corn.[31] According to Corn, "Defend Forward is meant to proactively contest, disrupt and degrade cyber aggression at or as close as practicable to its source before it reaches U.S., allied, and partner networks. It takes as a given adversary persistence and entrenched will and is, therefore, aimed

principally at disruption, not dissuasion."[32] Corn further explained why deterrence does not work in cyberspace: "Given the physical, virtual and normative structure of cyberspace, the strategic incentives for adversaries to engage in hostile cyber operations—at least those not clearly crossing the use-of-force threshold—so significantly outweigh the disincentives that traditional deterrence models hold little to no sway."[33] The failure of deterrence (regardless of actual or merely perceived) in cyberspace inspires support for a more proactive cyber posture through PE and DF frameworks.

Relevant Publications

This paper draws upon cyber strategy literature and publications to explain why the United States should continue implementing PE and DF in future cyber strategies. Two leading schools of thought exist within the body of unclassified, peer-reviewed literature dedicated to this topic: those who argue the 2018 Strategy will produce favorable tactical, operational, and strategic effects for the United States, and those who argue that it will create a dangerous escalation in cyberspace by amplifying reactionary actions on the conflict continuum.[34] In general, scholars believe that PE and DF frameworks are either effective or ineffective.

The Army Cyber Institute's (ACI) Cyber Defense Review (CDR) publishes some of the most significant ideas supporting PE and DF. In the Spring 2020 CDR, James R. Platte wrote an article titled "Defending Forward on the Korean Peninsula."[35] In it, he argued PE and DF could effectively be used to reduce North Korea's malicious cyber activity. Platte's article places these frameworks within an operational as well as a strategic context. COL (ret) Corn – who holds Director of ACI amongst his many former titles – reinforces Platte's position by arguing in favor of the legality of U.S. presence on foreign networks.[36] Corn's article in the *Temple International*

& Comparative Law Journal in 2018 titled "The Use of Force and Cyber Countermeasures" details how cyber measures are far more challenging to implement than traditional methods of force, arguing that restrictions to offensive cyber operations must be relaxed in order to defend in cyberspace effectively.[37]

Policymakers have further shaped cyber strategy debate through a significant number of public statements. The shift in some policymakers' perspectives is a reflection of the dynamic nature of this debate. One example of this is Emily Goldman, a prominent cyber strategist and member of the Policy Planning Staff at the Department of State. At an American Bar Association panel of lawyers in November 2019, she shared her perspective that the 2018 Strategy will prove ineffective against state actors like China.[38] However, by the Fall of 2020, her viewpoint had changed. Goldman's article in Texas National Security Review revealed her new opinion that the U.S. needed to pursue PE and DF.[39] Goldman's bit flip is just one example of the many such shifting perspectives amongst policymakers today.

One leader who has not shifted perspective is the NSA/CSS/USCC Commander, GEN Nakasone. In a 2019 *Joint Forces Quarterly* article, he argued that the United States must effectively defend forward in cyberspace or risk falling behind its adversaries.[40] Similarly, American political theorist and founder of neoliberalism Joseph S. Nye published an article in the *MIT Press Journal* called "Deterrence and Dissuasion in Cyberspace," where he explained the mechanisms by which cyber can be effectively used for strategic deterrence and denial.[41] These articles clearly and convincingly argue the United States must maintain technological pace with its adversaries during the current Revolution in Military Affairs (RMA).

This body of literature in favor of more restrictions on U.S. cyber strategy is more developed than in favor of a proactive strategy. This disparity is likely because the idea of a

proactive national cyber strategy is newer than the concept of a defensive approach. Amongst scholars who argue that U.S. cybersecurity strategy should be more restrictive, there are two sub-groups: those who merely believe PE and DF will be ineffective and those who believe these frameworks will prove detrimental to U.S. strategic interests. The former group is smaller and includes influential voices such as Marietje Schaake, President of the CyberPeace Institute and a policy director at Stanford University. In a recent article in Foreign Affairs magazine, Schaake argued that the United States needs to have much more oversight of cyber offensive and defensive operations. Her article highlights the gaps between private and public sector capabilities and calls for a greater convergence of efforts. Similarly, David Mussington, Director of the Center for Public Policy and Private Enterprise at the University of Maryland, focuses his arguments against PE and DF on the lack of public-private sector data sharing.[42] Mussington goes one step further than Schaake by arguing that these frameworks could create a deleterious new norm for state cyber actions, which would reduce global stability.[43]

Scholars who have argued that PE and DF are merely ineffective include Jason Healey, Neil Jenkins, and JD Work. Healy's prolific publications on cyber deterrence include one article from the *Journal of Cybersecurity* titled "The Implications of Persistent (and Permanent) Engagement in Cyberspace," which argues that PE and DF will fail to deter adversary cyber activities because these frameworks are based on an improbable series of assumptions and circumstances.[44] Similarly, Jason Healey and Neil Jenkins published an article for CyCon 2020 called "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing." This article argues that it is too soon to quantifiably identify whether or not the 2018 Strategy is working, and it offers a metrics-based framework for examining future effectiveness. Finally, Healey, Jenkins,' and JD Work's article for CyCon 2020 called "Defenders Disrupting

Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations" builds upon Healey's and Jenkins' previous work by further delineates specific metrics and case studies for successful cyber operations.[45]

Finally, a growing group of scholars favor a more passive, normative approach to cyber strategy. In September 2019, Eneken Tikk and Mika Kerttunen published an article in the *Norwegian Institute of International Affairs Journal* called "Parabasis: Cyber Diplomacy in Stalemate." This article argues that the United States' current cyber strategy risks sparking antagonistic actions: cyber policy should instead be driven by forming international norms.[46] More recently, Ducheine and Pijpers published a paper through the Amsterdam Center for International Law titled "The Mission Component in Deterrence Theory: The Legal Framework." They concur with Tikk and Kerttunen's opinion that a legal framework must be established before embarking on significant cyber deterrence operations.[47]

Within the group of scholars opposed to PE and DF, three final scholars warrant mention due to their influential voices against this strategic approach. First, Brandon Valeriano and Benjamin Jensen's article "The Myth of the Cyber Offense" in *CATO Institute's Policy Analysis Journal* in January 2019 argues that offensive national cyber strategies are not merely strategically ineffective, but also dangerously alter current norms, paving the way for an unnecessary escalation of force. Drawing from Valeriano and Jensen's work, British scholar Mariarosaria Taddeo published an article titled "Norms and Strategies for Stability in Cyberspace" in the *Italian Institute for International Political Studies Report*. In this, she argues that without a framework of norms and strategies, cyberspace will become an irreparable "wild west."[48]

Within the body of literature on U.S. cybersecurity strategy, PE and DF have shaped recent domestic and international cybersecurity debates. Scholars generally fall into two groups – those in favor of the 2018 Cyber Strategy and its primary frameworks of PE and DF, and those opposed to this strategic approach. These arguments are colored by the recent advent of cyberspace itself, the lack of international cyber laws and norms, and the dynamic nature of domestic and international cyber strategy.

Military Reasons

The 2019 NDAA's reclassification of cyberspace operations as TMA enabled PE and DF to assume an active, operational military role supporting existing strategic military guidance. PE and DF support the most recent National Security Strategy (NSS), National Defense Strategy (NDS), and National Military Strategy (NMS) by enabling proactive cyber operations capable of defense, denial, degradation, disruption, and defeat – all below the level of armed conflict.

At the highest level of strategic guidance, the 2017 NSS states that the United States will "defend, and when necessary defeat malicious actors who use cyberspace capabilities against the United States… [the US] will be risk informed, but not risk-averse, in considering [its] options."[49] Significantly, the 2017 NSS' approach to risk is a shift from previous strategies, which took a more cautious and reactive approach to operational risk: in the 2015 NSS, President Obama intended merely to "pursue a comprehensive agenda that draws on all elements of our [U.S.] national strength, that is attuned to the strategic risks and opportunities we face...."[50] PE and DF implement the 2017 guidance to pursue a risk-informed cyber strategy by introducing new operational interactions within agreed competition short of war.[51]

Nested directly under the NSS, the 2018 NDS states that DOD's actions enable diplomatic negotiations from a position of strength, but if diplomacy and deterrence fail, the Joint Force will take military actions to win.[52] Within cyberspace, the NDS explains the United States will "prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable [the United States] to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks." [53] In support of the NDS, PE and DF encompass military actions to defend against and deny advantages to adversaries in cyberspace *during a cyberattack*. Notably, the 2018 USCC *Command Vision* notes that "well defended cyber terrain is attainable but continually at risk."[54] Moreover, timely proactive cyber actions within agreed competition allow the United States strong diplomatic positions from which to negotiate by both facilitating attribution of adversary actions in cyberspace and acquiring forward operational footholds for a potential counterattack.

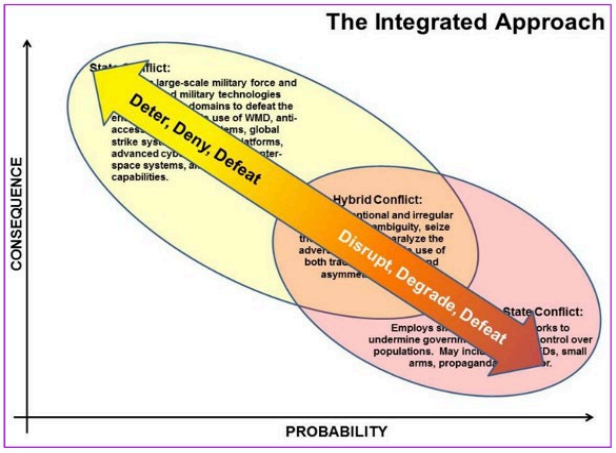

Figure 1: Integrated Approach to the Continuum of Conflict

Finally, the 2018 NMS includes a new mission focus of "[competing] below the level of armed conflict (with a military dimension)."[55] The previous NMS, published in 2015, provided a framework for an integrated approach to the conflict continuum in which deterrence, denial, and defeat were the preferred strategies for high consequence/low probability threats, and disruption, degradation, and defeat were the strategies for low consequence/high probability threats (Figure 1). The 2018 NMS notably approaches cyber threats more proactively with the added mission focus area of military competition short of

armed conflict. PE and DF frame the operational disruption of adversary cyber actions and degradation of adversary cyber capabilities even in low probability/high consequence situations, thereby supporting the shift from the 2015 to the 2018 NMS. Overall, PE and DF directly support strategic guidance in the 2017 NSS, the 2018 NDS, and the 2018 NMS.

One way in which PE and DF do not directly fulfill the strategic goals of the NSS, NDS, and NMS is through deterrence. Many scholars mistakenly assume that these frameworks are primarily deterrence strategies. Some even use the assumption that PE and DF are deterrence strategies as the basis for scholarly arguments: for example, the prominent cybersecurity scholar Jason Healey recently articulated that PE and DF are not reliable means of deterring adversary behavior.[56] In their widely-read paper for the CATO Institute, Valeriano and Jensen further argue that proactive cyber offensive actions are flawed because they are ineffective at preventing attacks from malicious actors.[57] They contend that PE and DF will escalate reactions within the cyber domain but fail to deter enemy attacks effectively.[58] However, as Jacqueline Schneider explains in an article on *Lawfare*, "[PE is] not as much an articulation of a new stand-alone strategy as it is a counterargument against the deterrence-based and norms-based strategies of the Obama administration."[59] Gary Corn concurs with Schneider's summary, explaining that neither of these strategic frameworks is intended for deterrence; instead, PE and DF's primary purpose lies primarily in *disruption*.[60] While PE and DF's primary purpose is not to deter, that does not mean PE and DF cannot contribute to deterrence over the long term. Deterrence can be a potential long-term benefit of PE and DF, but it is not the primary purpose of these strategic frameworks.

In fact, the two main frameworks of the current U.S. cyber strategy are predicated upon the idea that it is too late to implement deterrence – they accurately assume that hostile actions in

cyberspace are already occurring routinely. According to the Joint Chiefs of Staff, "Deterrence operations convince adversaries not to take actions that threaten U.S. vital interests by means of decisive influence over their decision-making."[61] But within cyberspace, nefarious state and non-state actors have already conducted this decision-making process – demonstrated through the relentless rate of cyberattacks against the United States. Adversaries have already penetrated U.S. networks and proven the desire, capability, capacity to act maliciously, below the level of armed conflict, against the United States. Therefore, it is too late to influence adversary decision-making in the short term. PE and DF frameworks acknowledge this strategic posture and therefore are not elements of a deterrence strategy.

Because it is too late to implement deterrence, the 2018 Strategy focuses on seizing the initiative through disruption.[62] According to Joint Publication 3-0 (Operations), "As operations commence, the JFC needs to exploit friendly advantages and capabilities to shock, demoralize, and disrupt the enemy immediately…. The JFC seeks decisive advantage through the use of all available elements of combat power to seize and maintain the initiative, deny the enemy the opportunity to achieve its objectives, and generate in the enemy a sense of inevitable failure and defeat."[63] The goal of seizing the initiative is to establish an environment conducive to deterrence. This shift in focus is portrayed in the lack of focus on the term "deter" in Joint Publication 3-12 (Cyberspace Operations); it is only found once – in a cited quote from the 2015 DoD Cyber Strategy.[64] PE and DF implement the Joint Chiefs' emphasis on denial in cyberspace by degrading adversary capabilities, disrupting adversary access, and destroying adversary access to cyber targets. These actions aim to regain the initiative within the agreed competition space and lay the foundation for an effective cyber deterrence strategy.

The PE and DF frameworks of cyber strategy also support the DoD's shift from counterterrorism operations to Great Power Competition (GPC) through realigning cyber planning from an event-driven process towards one focused on long-term objectives integrating the whole-of-government approach (WGA). Before 2018, cyber planning methodology followed a more traditional process based on the Joint Planning Process (JPP). Cyber planning drew from the JPP for three primary reasons. First, the evolving nature of cyber operations made it difficult to implement a new process while USCC was still forming. Second, the NCA required for offensive cyber operation approval remained undelegated, so few operations were occurring. Third, the lack of WGA-integration led to DoD-constrained cyber planning. However, the JPP posed several problems for cyberspace operations planners. Most significantly, it required a clearly defined mission, an unrealistic understanding of the adversary, and an impossible standard for Measures of Performance and Effectiveness. While the PE and DF frameworks are not planning processes, they *are* operational approaches that necessitate a fresh approach to strategic cyberspace planning.

The USCC-led Joint Task Force-Ares (JTF-Ares) laid the groundwork for just such a new planning approach. Established in 2016, JTF-Ares created a new framework for cyber-focused integration amongst multiple government stakeholders. However, it still focused on counterterrorism missions and operated under existing Authorizations for Use of Military Force (AUMFs). Two years later, GEN Nakasone publicly announced the Russia Small Group (RSG). The RSG built upon the JTF-Ares model, but furthered it by seamlessly integrating more government entities and creating a mission set aligned against a near-peer, nation-state competitor below the level of armed conflict.

In response to the recent SolarWinds attacks, the U.S. Government announced a further adaptation of this model – the Cyber Unified Coordination Group (UCG). Led by the National Security Council, the UCG focuses on identifying the scope and potential mitigation methods of the SolarWinds attack across both public and private sectors.[65] This significant shift in cyberspace operations planning – a direct result of the strategic frameworks of PE and DF – capitalized on the improved understanding of the nature of cyber operations, the delegated approval authorities for cyber operations, and the increased channels for a WGA to cyberspace planning operations. It propelled cyber planning efforts from singular, event-driven processes rooted in the JPP to long-term efforts across the conflict continuum, thereby supporting the greater DoD shift from counterterrorism to GPC.

The United States must continue to employ a PE- and DF-centered cyber strategy to support strategic guidance on DoD operations and necessitate an improved planning process focused on GPC. PE and DF support the shift in military operations towards GPC by implementing cyber defense, denial, degradation, disruption, and defeat, while regaining the initiative required to implement future military deterrence in cyberspace. Because of this, PE and DF represent vital military frameworks for future cyberspace operations.

Economic Reasons

If the United States fails to maintain the initiative, it will be caught focusing on cyber defense. As proven by efforts before 2018, a defense-focused cyber strategy is ineffective at protecting national interests and deterring adversary behavior. Not only does a defensive cyber posture result in a disadvantageous military and political posture, but it also imposes exorbitant

costs. Failing to continue implementing PE and DF poses financial risks that threaten to cripple the U.S. economy.

Cyberattacks can cause fiscal damage in three ways. First, they can directly steal IP, which took years of research and development to obtain. The United States has repeatedly seen its technologies, data, and information stolen by adversaries in cyberspace – all below the threshold of armed conflict. As the world leader in innovation, the United States is also the primary target for IP theft. As SASC member Senator Rounds analogized, much like a mouse stealing a piece of cheese (or a missile hitting American soil), by the time the crime is committed it is far too late to mitigate or repair the damage. One prominent example of IP theft is the case of the F-35s.[66] This case is noteworthy because it targeted the U.S. Defense Industrial Base. China not only stole research and development time in the form of F-35 plans, but it also gained a strategic advantage in military weaponry. While it is impossible to accurately assess the value of the F-35 theft because the ramifications continue to evolve, economic analysts have developed rough numbers for the costs of IP theft to the U.S. economy: a 2017 report by the Bureau of Asian Research's Commission on the Theft of American Intellectual Property notes that the annual cost (to the U.S. economy) of IP theft to was between $225 and $600 billion dollars.[67]

The second way attacks incur fiscal damage consists of first- and third-party costs to the attacked entity.[68] First-party costs include those that result directly from the incident. These include malicious code investigation and cleanup, immediate software purchases needed to patch the hacks, man-hours devoted to addressing the hacks, reacting to the situation, and incorporating further safety protocol patches, adverse effects on the company's public reputation and share price, and customer support efforts. Third-party costs include those costs resulting from private litigation. Unfortunately, accurately assessing the costs of cyberattacks is difficult due to

inadequate data. Sasha Romanosky explains how cyber incidents become observed, public data, and are subsequently incorporated into economic estimates (Figure 2).[69] Despite the lack of data, statistical analysis done by Romanosky, which incorporates information from insurance payouts and other sources, indicates that the average cost of a data breach is around $6.5 million.[70] Data breaches – which along with security incidents, privacy violations, and phishing and identity thefts, comprise one of four types of cyberattacks – are increasing in both frequency and cost per incident.

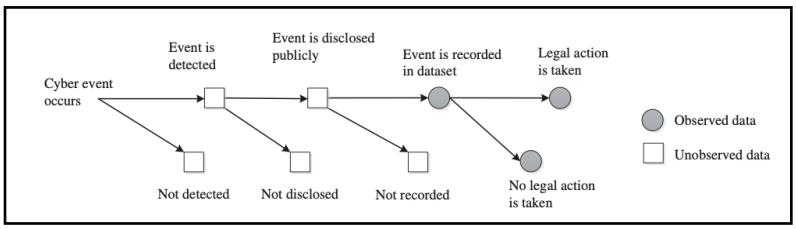

Figure 2: Data Generating Process for Cyberattacks

In 2018, the U.S. Council of Economic Affairs (CEA) published a report titled "The Cost of Malicious Cyber Activity to the U.S. Economy." This report explains that professional cybersecurity costs to the economy per incident for a cyberattack range from $2.7 million to $498 million. As it is impossible to correlate precise geographic origins to these costs, this number represents the cost to the American economy of aggregate, geographic-agnostic, malicious activity. For 2016, CEA found that firms lost approximately 0.8% of their market share within a week of a public announcement of a cyber event.[71] A recent and germane example of this is the SolarWinds attack.[72] As noted by the IT-focused news source CRN recently: "Cyber insurance vendors are expected to spend $90 million on incident response and forensic services for clients who were compromised by the SolarWinds hackers."[73] Also, SolarWinds stock itself dropped due to the public pronouncement of the hack: SWI stock (SolarWinds stock, traded on the New York Stock Exchange) went from $23.55 per share on December 11, 2020 to $14.18 per share on December 18, 2020 – nearly a 40% drop in share price. Furthermore, attacks

have been steadily increasing: according to PurpleSec, a cybersecurity firm, the total number of malware infections reported in the United States in 2009 was 12.4 million; in 2018, it was 812.67 million.[74]

The third way cyberattacks can cause fiscal damage is through the loss of public faith in the system. Cyberattacks are inherently breaches of trust and have reverberating effects on individual perceptions, which shape future behavior. As one cybersecurity company notes, when a cyberattack occurs, "the credibility of government institutions is jeopardized, causing even greater inflation of resources used to overcome such damaging fiscal setbacks."[75] Cyberattacks can cause fiscal damage far beyond quantifiable and documented costs – they can disrupt American society by eroding the fabric of its governmental system.

A common argument against PE and DF frameworks promotes an increased cyber defense network instead of proactive engagement. However, this argument fails to understand basic computing characteristics. A refresher on two basic trend prediction frameworks – Moore's Law and Metcalf's Law – easily repudiates this argument. Moore's Law, written by Intel co-founder Gordon Moore in 1965, states that the density of transistors – those basic switches in computing that enable the speed of connectivity - would double every two years. Almost three decades later, George Gilder took a slide from one of Metcalf's presentations and extrapolated the idea to state that network value is proportional to N^2.[76] In English, this means because the value of a network is proportional to the number of nodes, and because the number of nodes is increasing exponentially, then the prevalence of networks will increase exponentially.

The timing of the new US Strategy could not be more critical – now, on the cusp of quantum computing and a subsequent boom in supercomputing capabilities, the idea of reactive network defense could increasingly result in global network isolation. Global network isolation

is not only anathema to the very culture and spirit of the American people, but it is also a poor economic strategy: such restrictions would simply drive businesses out of the United States. In short, because of the nature of cyberspace, focusing on restraint would be similar to creating a modern-day Maginot Line – something cybersecurity firms identified years ago, as seen in FireEye's report from 2015 titled, "Maginot Revisited: More Real-World Results from Real-World Tests." In this report, the prominent cybersecurity firm FireEye recommended a shift in cybersecurity approaches, arguing that companies need to "move away from passive, poorly integrated defenses that provide a fragmented view of threats and cannot connect the dots in advanced attacks… [they need] a tightly integrated, nimble architecture that enables big-picture vigilance."[77] The report goes on to note that, "today's security organizations can't afford to passively wait for attacks…instead, they should take a lean-forward approach that actively hunts for new and unseen threats."[78] This verbiage is a significant harbinger of similar phrasing used in the planning and implementation of the 2018 Cyber Strategy.

Strategic Reasons

Strategic planning differs from military planning. As former Secretary of State Dean Acheson explained, strategic planning is "to look ahead, not into the distant future, but beyond the vision of the operating officers caught in the smoke and crises of current battle; far enough ahead to see the emerging form of things to come and outline what should be done to meet or anticipate them."[79] It is not enough for the U.S cyber strategy to be effective for immediate military or economic purposes, but it must also provide lasting benefits without deleterious repercussions.

As an increasing number of states gain sophisticated capabilities and capacity within cyberspace, a framework for normative behavior will need to emerge to mitigate potential fallout from hostile actions or escalatory behavior.[80] There are two ways in which PE and DF frameworks enable the creation of a favorable set of norms in cyberspace. The first is through tacit bargaining. The second is by increasing the connective tissue within the federal government, which will support the creation of norms through litigious means. Cyber is a new domain (and the only artificial domain), and the innovations involved poise our world on the edge of an RMA.[81] The United States has been reticent to enter into the legal fray of cyberspace, but DoD's efforts will normalize proactive cyber operations between states and open the door for litigation to forge new norms.

In contrast to the explicit bargaining used in previous cyber strategies, PE and DF frameworks implement norms in cyberspace through tacit bargaining. Explicit bargaining in cyber has been attempted a few times. The most prominent examples were during the Obama administration, where the United Nations 2013 and 2015 Group of Governmental Experts (GGE) attempted to promote a list of voluntary norms for operating in cyberspace; in 2017, these efforts stalled due to a lack of buy-in from UN nations.[82] Another example is the 2015 Obama-Xi agreement, which attempted to curtail IP theft.[83] This agreement failed to curb behavior because it lacked both positive and negative incentive structures.

As far as a negative incentive structure, attribution remains the lynchpin in cyberspace. While a state may be aware of an adversary's presence on its network, little can be done about this presence until the state can publicly attribute nefarious actions to this adversary. Public attribution is difficult to achieve without exposing a state's tactics, techniques, procedures, and accesses. Few incentives exist for altruistic behavior within cyberspace. As explained through

the mouse metaphor – the mouse is attracted to the warmth and the food in the house; only the very small risk of being caught disincentivizes the mouse from attempting to gain these things. The only potential incentive for a state also hinges on attribution, and it is less of a carrot and more of a fear of loss. If the offended state exposes the aggressor state to the global community, this can erode the global perception (or moral high ground) of the aggressor state, subsequently eroding its global bargaining power. However, again, this requires the offended state to show its hand, potentially at the cost of exposing classified collection capabilities.

When it comes to tacit bargaining, which essentially creates norms through actions instead of verbal agreements, the PE and DF frameworks offer an effective operational strategy in cyberspace. Tacit bargaining depends on a body of experience – patterns of actions.[84] This type of bargaining lends itself well to cyberspace, in which malicious actors and malware are primarily codified by patterns of behavior. According to Fischerkeller and Harknett, tacit bargaining can create reliable expectations of behavioral norms within cyberspace.[85] Forward, continuous cyber operations will enable the United States to build the scaffold of internationally accepted behavior.

Finally, the United States must continue PE and DF to enable the development of a normative framework through litigious mechanisms. As Martha Finnemore argues in her book, "The Purpose of Intervention: Changing Beliefs About the Use of Force," International Human Rights Law can be informed through the actions of lawyers themselves.[86] Finnemore points out that discussions between lawyers resulting in minor legal determinations can constitutively swell, eventually affecting the greater community through a regulative framework. As private companies are already much further along than governments with creating norms through constitutive ontological effects (as seen with the Cyber Peace Institute and the Cybersecurity

Tech Accords), the U.S. Government could support norms deterring malicious actors by choosing to weigh in on cybersecurity cases. Pushing cyberlaw cases through the system will create a new normative standard within the United States; it will not take long to spread internationally. PE and DF frameworks require a WGA, enabling norms-through-litigation efforts by forging the connective tissue within the Federal Government to deal with nuanced cybersecurity cases effectively.

Conclusion

Persistent Engagement and Defend Forward, the two main frameworks of the 2018 Cyber Strategy, represent a bit flip in the U.S. approach to cyberspace. While they do not exist in a silo – they are buttressed by considerable intra-governmental efforts to enable, including revisions to terminology and increased funding – they constitute the most significant shift in U.S. cyber strategy to date. Implementing these frameworks is crucial because they enable operationally sound military actions to maintain the initiative and directly support the National Security Strategy, National Defense Strategy, and National Military Strategy. Economically, they allow the United States to prevent Intellectual Property theft, reduce cyberattacks and subsequent costs, and maintain the trust of the American public. Strategically, these frameworks enable the development of norms through tacit bargaining and developing a legal framework for cyberspace. It is worth echoing the benefits of these frameworks to ensure the current Presidential administration continues to persistently and proactively engage with adversaries in cyberspace in order to defend the nation.

Endnotes

[1] *Statement of General Paul M. Nakasone: Hearing before the House* Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, 116th Cong., 3 (2020) (statement of General Paul M. Nakasone, Commander, United States Cyberspace Command). https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.
[2] Paul Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly Issue 92* (2019), 10-14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.
[3] C. Todd Lopez, "Persistent Engagement, Partnerships, Top Cybercom's Priorities," *Defense.gov*, May 14, 2019, https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.
[4] Glenn Alexander Crowther, "The Cyber Domain," *The Cyber Defense Review* 2, no. 3 (2017), 63-78, http://www.jstor.org/stable/26267386.
[5] National Initiative for Cybersecurity Careers and Studies, Cybersecurity Glossary, "Cyberspace," accessed January 19, 2021, https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.
[6] National Initiative for Cybersecurity Careers and Studies, Cybersecurity Glossary, "Cybersecurity."
[7] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff, June 8, 2018), vii, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[8] Catherine A. Theohary, *Defense Primer: Cyberspace Operations,* CRS Report for Congress IF10537 (Washington DC: Congressional Research Service, December 15, 2020), https://fas.org/sgp/crs/natsec/IF10537.pdf.
[9] Catherine A. Theohary, *Defense Primer: Cyberspace Operations.*
[10] Ibid.
[11] Ibid.
[12] Gary Corn, "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse," *Lawfare* (blog), January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
[13] C. Todd Lopez, "Persistent Engagement, Partnerships, Top Cybercom's Priorities," *Defense.gov*, May 14, 2019, https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.
[14] Gary Corn, "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse," *Lawfare* (blog), January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
[15] Gary Corn, "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse."
[16] Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare (blog)*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.
[17] JD Work, "Insecurity, Capabilities Acquisition, and Conflict," (class lecture, Cyber Operations, Intelligence and Conflict, Marine Corps University, Quantico, VA January 15, 2021).
[18] U.S. Executive Office of the President, *International Strategy for Cyberspace*, (Washington, DC, May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[19] U.S. Department of Defense, *Strategies for Operating in Cyberspace*, (Washington, DC, July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
[20] Center for Strategic & International Studies, "Significant Cyber Incidents Since 2006," accessed January 19, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[21] Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare (blog)*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.
[22] Denise E. Zheng, "Critical Questions: 2015 DoD Cyber Strategy," *Center for Strategic & International Studies* (website), April 24, 2015, https://www.csis.org/analysis/2015-dod-cyber-strategy.
[23] U.S. Cyberspace Solarium Commission Report (March 2020), https://www.solarium.gov/report.
[24] Mark Pomperleau, "Two Years In, How Has a New Strategy Changed Cyber Operations?" *Fifth Domain*, November 11, 2019, https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/.
[25] Mark Pomperleau, "It's a New Era for Cyber Operations, but Questions Remain," *Fifth Domain*, September 28, 2018, https://www.fifthdomain.com/dod/2018/09/28/its-a-new-era-for-cyber-operations-but-questions-remain/.

[26] Mark Pomperleau, "It's a New Era for Cyber Operations, but Questions Remain."
[27] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis*, vol 61, no. 3 (2017) 381-393, https://doi.org/10.1016/j.orbis.2017.05.003.
[28] U.S. Executive Office of the President. *National Cyber Strategy of the United States of America*, (Washington, DC, September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[29] Mark Pomperleau, "Two Years In, How Has a New Strategy Changed Cyber Operations?" *Fifth Domain*, November 11, 2019, https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/.
[30] JD Work, "Insecurity, Capabilities Acquisition, and Conflict," (class lecture, Cyber Operations, Intelligence and Conflict, Marine Corps University, Quantico, VA January 15, 2021).
[31] Gary Corn, "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse," *Lawfare* (blog), January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
[32] Gary Corn, "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse."
[33] Ibid.
[34] Jason Healey, "Triggering the New Forever War, in Cyberspace," *The Cipher Brief*, April 2018, https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace; and Max Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security Vol. 35 (February 11, 2018)*, 444-453, https://doi.org/10.1080/02684527.2020.1729316.
[35] James R. Platte, "Defending Forward on the Korea Peninsula," *Cyber Defense Review* 5 No. 1 (2020), 75-94, accessed March, 30, 2021, https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2006_Platte_WEB.pdf.
[36] Rick Weber, "DoD'S 'Defend Forward' Cyber Strategy Prompts Lively Debate by ABA," *Inside the Pentagon's Inside the Army 31, No. 46* (November 18, 2019), https://search-proquest-com.lomc.idm.oclc.org/trade-journals/dods-defend-forward-cyber-strategy-prompts-lively/docview/2315038968/se-2?accountid=14746.
[37] Gary Corn and Eric Talbot Jensen, "The Use of Force and Cyber Countermeasures" 32 Temple International & Comparative Law Journal 127 (2018), BYU Law Research Paper No. 18-18, accessed March 30, 2021. https://ssrn.com/abstract=3190253.
[38] Rick Weber, "DoD'S 'Defend Forward' Cyber Strategy Prompts Lively Debate by ABA," *Inside the Pentagon's Inside the Army 31, No. 46* (November 18, 2019), https://search-proquest-com.lomc.idm.oclc.org/trade-journals/dods-defend-forward-cyber-strategy-prompts-lively/docview/2315038968/se-2?accountid=14746.
[39] Emily Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," Texas National Security Review (September 3, 2020), http://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/.
[40] Paul Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly Issue 92* (2019), 10-14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.
[41] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security 41, No. 3* (January 2017), 44–71, https://doi.org/10.1162/ISEC_a_00266.
[42] Rick Weber, "DoD'S 'Defend Forward' Cyber Strategy Prompts Lively Debate by ABA," *Inside the Pentagon's Inside the Army 31, No. 46* (November 18, 2019), https://search-proquest-com.lomc.idm.oclc.org/trade-journals/dods-defend-forward-cyber-strategy-prompts-lively/docview/2315038968/se-2?accountid=14746.
[43] Rick Weber, "DoD'S 'Defend Forward' Cyber Strategy Prompts Lively Debate by ABA."
[44] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity Vol 5 No. 1* (2019), https://doi.org/10.1093/cybsec/tyz008.
[45] Jason Healey, Neil Jenkins, and JD Work, "Defender Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations," *12th International Cyber Conference* (2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf.
[46] Eneken Tikk and Mika Kerttunen, "Parabasis: Cyber-Diplomacy in Stalemate," *Norwegian Institute of International Affairs* (2018), 88, http://hdl.handle.net/11250/2569401.
[47] P.A.L. Ducheine and Peter Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework" *Amsterdam Law School Research Paper No. 2020-70* (December 14, 2020), Amsterdam Center for International Law No. 2020-34, https://ssrn.com/abstract=3748348 or http://dx.doi.org/10.2139/ssrn.3748348.

[48] Mariarosaria Taddeo, "Norms and Strategies for Stability in Cyberspace," *ISPI – Report: The Global Race for Technological Superiority: Discover the Security Implications* (April 25, 2020), https://ssrn.com/abstract=3585082 or http://dx.doi .org/10.2139/ssrn.3585082.
[49] White House, *National Security Strategy of the United States of America December 2017* (Washington, DC, 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[50] White House, *National Security Strategy February 2015* (Washington, DC, 2015), https://nssarchive.us/wp-content/uploads/2020/04/2015.pdf.
[51] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *Institute for Defense Analysis* (May 2018), 273, https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.
[52] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge* (Washington, DC, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[53] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge*.
[54] U.S. Cyber Command, *U.S. Cyber Command Vision: Achieve and Maintain Cyberspace Superiority* (April 20, 2018), 4, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
[55] Joint Chiefs of Staff, *Description of the 2018 National Military Strategy 2018* (Washington, DC, 2018), https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf.
[56] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity Vol 5 No. 1* (2019), https://doi.org/10.1093/cybsec/tyz008.
[57] Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," *CATO Institute Policy Analysis No. 862* (January 15, 2019), https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.
[58] Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint."
[59] Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare (blog)*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.
[60] Gary Corn, "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse," *Lawfare* (blog), January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
[61] U.S. Department of Defense, *Deterrence Operations Joint Operating Concept* (Version 2.0, December 2006), 8, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337.
[62] Joint Chiefs of Staff, *Joint Operations*, JP 3-0 (Washington, DC: Joint Chiefs of Staff, October 22, 2018), xxiii, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.
[63] Joint Chiefs of Staff, *Joint Operations*, JP 3-0.
[64] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff, June 8, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[65] Katya Maruri, "Federal Task Force Will Investigate Russia-Led Cyberattack," *Govtech.com*, January 12, 2021, https://www.govtech.com/security/Federal-Task-Force-Will-Investigate-Russia-Led-Cyberattack.html.
[66] Mike O'Brien, "Pentagon Admits F-35 Data Theft is a Major Problem," *Institute for Defense and Government Advancement*, June 20, 2013, https://www.idga.org/archived-content/news/pentagon-admits-f-35-data-theft-is-a-major-problem.
[67] Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Washington, DC, February 2017), https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.
[68] Sarah Romanosky, "Examining the Costs and Causes of Cyber Incidents," *Journal of Cybersecurity Vol 2* (2016), 129, https://academic.oup.com/cybersecurity/article/2/2/121/2525524.
[69] Sarah Romanosky, "Examining the Costs and Causes of Cyber Incidents."
[70] Ibid.
[71] U.S. Executive Office of the President, Council of Economic Advisors, "The Cost of Malicious Cyber Activity for the U.S. Economy," February 2018, 8, https://www.hsdl.org/?view&did=808776.

[72] Kari Paul, "What You Need to Know About the Biggest Hack of the U.S. Government in Years," *The Guardian*, December 15, 2020, https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department.
[73] Michael Novinson, "SolarWinds Hack Could Cost Insurance Firms $90 Million," *CRN.com*, January 14, 2021, https://www.crn.com/news/security/solarwinds-hack-could-cost-cyber-insurance-firms-90-million#:~:text=and%20Technology%20Integrators,SolarWinds%20Hack%20Could%20Cost%20Cyber%20Insurance%20Firms%20%2490%20Million,%2C'%20says%20BitSight's%20Samit%20Shah.
[74] Purplesec, "Cyber Security Statistics," *Purplesec.us* (website), accessed January 19, 2021, https://purplesec.us/resources/cyber-security-statistics/#:~:text=In%202018%20there%20were%2080%2C000,30%20million%20attacks%20per%20year.
[75] KnowBe4, "Cyber Attacks on Municipalities," *Knowbe4.com* (website), 2020, 3, https://www.knowbe4.com/hubfs/ Cyber-Attacks-on-Municipalities-White-Paper.pdf.
[76] Robert Metcalf, "It's All in Your Head," *Forbes*, April 20, 2007, https://www.forbes.com/forbes/2007/0507/052.html?sh=5966a42b47d3.
[77] FireEye, "Maginot Revisited: More Real-World Results from Real-World Tests," *FireEye.com,* accessed January 19, 2021, 21, https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-maginot-revisited.html#:~:text=from%20Re...-,Maginot%20Revisited%3A%20More%20Real%2DWorld%20Results%20from%20Real%2DWorld,swath%20of%20industries%20and%20geographies.&text=By%20design%2C%20any%20threat%20observed,through%20all%20other%20security%20defenses.
[78] FireEye, "Maginot Revisited: More Real-World Results from Real-World Tests."
[79] Dean Acheson, Present at the Creation (New York: W. W. Norton, 1969), 214.
[80] Emilio Iasiello, "What Happens if Cyber Norms Are Agreed To," *Georgetown Journal of International Affairs Fall/Winter 2016 Vol XVII, No III* (2016), 30, https://muse.jhu.edu/article/649446.
[81] Dorothy E. Denning, "Rethinking Cyber Domain and Deterrence," *Joint Force Quarterly No* 77 (April 1, 2015), https://ndupress.ndu.edu/Media/News/Article/581864/rethinking-the-cyber-domain-and-deterrence/#:~:text=This%20is%20reflected%20in%20the,former%20Director%20of%20the%20National.
[82] Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" *Lawfare (blog)*, July 4, 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.
[83] U.S. Office of the Press Secretary of the White House, "Fact Sheet: President Xi Jingping's State Visit to the United States," *The Obama White House Archives*, September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[84] Thomas C. Schelling, "Reciprocal Measures for Arms Stabilization," *Daedalus 134* (2005), 101-117, http://nrs.harvard.edu/urn-3:HUL.InstRepos:342594.
[85] Michael P. Fischerkeller and Richard J. Harknett, "What is Agreed Competition in Cyberspace?" *Lawfare (blog),* February 19, 2019, https://www.lawfareblog.com/what-agreed-competition-cyberspace.
[86] Martha Finnemore, *The Purpose of Intervention: Changing Beliefs About the Use of Force* (Ithaca, NY: Cornell University Press, 2003), http://www.jstor.org/stable/10.7591/j.ctt24hg32.

Bibliography

Acheson, Dean. *Present at the Creation*. New York, NY: W. W. Norton, 1969.

Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* 26 No. 3 (July 3, 2017). https://doi.org/10.1080/09636412.2017.1306396.

Brantly, Aaron. "The Cyber Deterrence Problem." *10th International Conference on Cyber Conflict CyCon X: Maximizing Effects* (2018). Accessed December 1, 2020. https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf.

Center for Strategic & International Studies. "Significant Cyber Incidents Since 2006." Accessed January 19, 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Chesney, Robert. "The Domestic Legal Framework for US Military Cyber Operations." *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2003* (July 29, 2020). https://www.lawfareblog.com/domestic-legal-framework-us-military-cyber-operations.

Commission on the Theft of American Intellectual Property. *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy.* Washington, DC, February 2017. https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.

Corn, Gary. "Solar Winds is Bad, but Retreat from Defend Forward Would be Worse." *Lawfare (blog).* January 14, 2021. https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.

Corn, Gary and Jensen, Eric Talbot. "The Use of Force and Cyber Countermeasures." (June 4, 2018). *32 Temple International & Comparative Law Journal 127* (2018), BYU Law Research Paper No. 18-18, https://ssrn.com/abstract=3190253.

Crowther, Glenn Alexander. "The Cyber Domain." *The Cyber Defense Review* 2, no. 3 (2017), http://www.jstor.org/stable/26267386.

Deeks, Ashley. "Defend Forward and Cyber Countermeasures." *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2004*, *Virginia Public Law and Legal Theory Research Paper No. 2020-59* (August 4, 2020). https://ssrn.com/abstract=3670896.

Denning, Dorothy E. "Rethinking Cyber Domain and Deterrence." *Joint Force Quarterly* No. 77 (April 2015). https://ndupress.ndu.edu/Media/News/Article/581864/rethinking-the-cyber-domain-and-deterrence/#:~:text=This%20is%20reflected%20in%20th e,former%20Director%20of%20the%20National.

Dobrygowski, Daniel. "Why Companies Are Forming Cybersecurity Alliances." *Harvard Business Review.* September 2019. https://hbr.org/2019/09/why-companies-are-forming-cybersecurity-alliances.

Doty, Kathleen. "The Emergence of Cyber Deterrence: Implications for International Law." *University of Georgia School of Law Legal Studies Research Paper No. 2018-08* (February 22, 2018). https://ssrn.com/abstract=3128578.

Ducheine, P.A.L. and Pijpers, Peter. "The Missing Component in Deterrence Theory: The Legal Framework." *Amsterdam Law School Research Paper No. 2020-70*, Amsterdam Center for International Law No. 2020-34 (December 14, 2020). https://ssrn.com/abstract=3748348 or http://dx.doi.org/10.2139/ssrn.3748348.

Farley, Robert. "Did the Obama-Xi Cyber Agreement Work?" *The Diplomat.* August 2018. Accessed December 1, 2020. https://thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/.

Finnemore, Martha. *The Purpose of Intervention: Changing Beliefs About the Use of Force*. Ithaca, NY: Cornell University Press, 2003. http://www.jstor.org/stable/10.7591/j.ctt24hg32.

FireEye. "Maginot Revisited: More Real-World Results from Real-World Tests." *FireEye.com.* Accessed January 19, 2021. https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-maginot-revisited.html#:~:text=from%20Re...-,Maginot%20Revisited%3A%20More%20Real%2DWorld%20Results%20from%20Real%2DWorld,swath%20of%20industries%20and%20geographies.&text=By%20design%2C%20any%20threat%20observed,through%20all%20other%20security%20defenses.

Fischerkeller, Michael P. "The Fait Accompli and Persistent Engagement in Cyberspace." *War on the Rocks.* Accessed June 24, 2020. https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/.

Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* Volume 61, Number 3 (2017). https://doi.org/10.1016/j.orbis.2017.05.003.

Fischerkeller, Michael P. and Richard J. Harknett. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." *Institute for Defense Analysis.* (May 2018). https://www.ida.org/-/media/feature/publications/p/pe/persistent-

engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.

Fischerkeller, Michael P. and Richard J. Harknett. "What is Agreed Competition in Cyberspace?" *Lawfare (blog)*. February 19, 2019. https://www.lawfareblog.com/what-agreed-competition-cyberspace.

Goldman, Emily. "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy." *Texas National Security Review* (September 3, 2020). http://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/.

Graff, Garrett M. "The Man Who Speaks Softly—and Commands a Big Cyber Army." *WIRED Magazine*. October 13, 2020. https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/.

Grigsby, Alex. "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased." *The Council on Foreign Relations*. November 2018. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Healey, Jason. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity*, Vol 5, No. 1 (2019), https://doi.org/10.1093/cybsec/tyz008.

Healey, Jason. "Triggering the New Forever War, in Cyberspace." *The Cipher Brief*. April 2018. https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace.

Healey, Jason, Jenkins, Neil, and Work, JD. "Defender Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations." *12th International Cyber Conferenc*e (2020). https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf.

Hoang, Lien. "Microsoft Helps Vietnam Fight Hackers Amid US-China Cloud Rivalry." *Nikkei Asia*. September 2020. https://asia.nikkei.com/Business/Technology/Microsoft-helps-Vietnam-fight-hackers-amid-US-China-cloud-rivalry.

Iasiello, Emilio. "What Happens if Cyber Norms Are Agreed To." *Georgetown Journal of International Affairs Fall/Winter 2016 Vol XVII, No III* (2016). https://muse.jhu.edu/article/649446.

International Institute for Strategic Studies. "Asia Pacific Regional Security Assessment 2019." *IISS*. May 2019. https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

Jiang, Min. “Cybersecurity Policies in China.” In *CyberBRICS: Cybersecurity Regulations in BRICS Countries,* edited by L. Belli, 195-212. Berlin, Germany: Springer, 2019. https://ssrn.com/abstract=3523325.

Joint Chiefs of Staff. *Cyberspace Operations*. JP 3-12. Washington, DC: Joint Chiefs of Staff, June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Joint Chiefs of Staff. *Description of the 2018 National Military Strategy 2018* (Washington, DC, 2018). https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf.

Joint Chiefs of Staff. *Competition Continuum.* Joint Doctrine Note 1-19. Washington, DC: Joint Chiefs of Staff, June 2019.

Joint Chiefs of Staff. *Joint Operations*. JP 3-0. Washington, DC: Joint Chiefs of Staff, October 22, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

Jones, Seth G. *Containing Tehran: Understanding Iran’s Power and Exploiting Its Vulnerabilities*. Center for Strategic and International Studies Transnational Threats Project (January 2020). https://www.csis.org/analysis/containing-tehran-understanding-irans-power-and-exploiting-its-vulnerabilities.

KnowBe4. “Cyber Attacks on Municipalities.” *Knowbe4.com* (website). 2020. https://www.knowbe4.com/hubfs/ Cyber-Attacks-on-Municipalities-White-Paper.pdf.

Levite, Ariel (Eli) and Jinghua, Lyu. “Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?” *Carnegie Endowment for International Peace* (January 2019). Additionally published in *China Military Science* (January 24, 2019). https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213.

Lopez, C. Todd. “Persistent Engagement, Partnerships, Top Cybercom’s Priorities.” *Defense.gov*. May 14, 2019. https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.

Maruri, Katya. “Federal Task Force Will Investigate Russia-Led Cyberattack.” *Govtech.*com, January 12, 2021. https://www.govtech.com/security/Federal-Task-Force-Will-Investigate-Russia-Led-Cyberattack.html.

Mazarr, Michael J. “Understanding Deterrence.” *RAND Perspectives* (April 2018). https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf .

Metcalf, Robert. “It’s All in Your Head.” *Forbes*, April 20, 2007. https://www.forbes.com/forbes/2007/0507/052.html?sh=5966a42b47d3.

Mitchell, A Wess. “The Case for Deterrence by Denial.” *TheAmericanInterest.*com. August 2015. https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/.

Nakasone, Paul. “A Cyber Force for Persistent Operations.” *Joint Forces Quarterly Issue 92* (2019). https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

National Initiative for Cybersecurity Careers and Studies, Cybersecurity Glossary. Accessed January 19, 2021. https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

Ney, Paul Jr. “DoD General Counsel Remarks at U.S. Cyber Command Legal Conference.” Speech. U.S. Cyber Command. March 20, 2020. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

Novinson, Michael. “SolarWinds Hack Could Cost Insurance Firms $90 Million.” *CRN.com*. January 14, 2021. https://www.crn.com/news/security/solarwinds-hack-could-cost-cyber-insurance-firms-90-million#:~:text=and%20Technology%20Integrators-,SolarWinds%20Hack%20Could%20Cost%20Cyber%20Insurance%20Firms%20%2490%20Million,%2C'%20says%20BitSight's%20Samit%20Shah.

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41 No. 3 (January 2017). https://doi.org/10.1162/ISEC_a_00266.

O’Brien, Mike. “Pentagon Admits F-35 Data Theft is a Major Problem.” *Institute for Defense and Government Advancement*, June 20, 2013. https://www.idga.org/archived-content/news/pentagon-admits-f-35-data-theft-is-a-major-problem.

O’Halloran, Joe. “US maintains Ban on Chinese Tech Firms as Huawei, ZTE Make 5G Leaps.” *Computer Weekly*. May 2020. Accessed December 1, 2020. https://www.computerweekly.com/news/252483155/US-maintains-ban-on-Chinese-tech-firms-as-Huawei-ZTE-make-5G-leaps.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. “Defense Science Board (DSB) Task Force on Cyber Deterrence.” February 23, 2017. https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf.

Paul, Kari. “What You Need to Know About the Biggest Hack of the US Government in Years.” *The Guardian*. December 15, 2020. https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department.

Platte, James R. “Defending Forward on the Korea Peninsula,” *Cyber Defense Review 5 No. 1* (2020). https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%20FULL_WEB.pdf.

Pomperleau, Mark. “It’s a New Era for Cyber Operations, but Questions Remain.” *Fifth Domain*, September 28, 2018. https://www.fifthdomain.com/dod/2018/09/28/its-a-new-era-for-cyber-operations-but-questions-remain/.

Pomperleau, Mark, “Two Years In, How Has a New Strategy Changed Cyber Operations?” *Fifth Domain*, November 11, 2019. https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/

Purplesec. “Cyber Security Statistics.” *Purplesec.us.* Accessed January 19, 2021. https://purplesec.us/resources/cyber-securitystatistics/#:~:text=In%202 018%20there%20were% 2080%2C000,30%20million%20attacks%20per%20year.

Ray, Charles A. “Cyberwar and Information Warfare: A Revolution in Military Affairs of Much Ado About not too Much?” Long essay, National War College, 1997. https://apps.dtic.mil/dtic/tr/fulltext/u2/a442714.pdf.

Reichert, Corinne. “US Finds Huawei Has Backdoor Access to Mobile Networks Globally, Report Says.” *CNet.com.* February 2020. https://www.cnet.com/news/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/.

Romanosky, Sarah. “Examining the Costs and Causes of Cyber Incidents.” *Journal of Cybersecurity Vol 2* (2016). https://academic.oup.com/cybersecurity/article/2/2/121/2525524.

Ropek, Lucas. “How Biden Could Change the Conversation on Cybersecurity.” *Government Technology (*blog). November 2020. https://www.govtech.com/security/How-Biden-Could-Change-the-Conversation-on-Cybersecurity.html.

SANS. “Advanced Persistent Threat (APT) and Insider Threat.” *SANS Cyber Defense* (blog). October 23, 2012. https://www.sans.org/blog/advanced-persistent-threat-apt-and-insider-threat/.

Schelling, Thomas C. “Reciprocal Measures for Arms Stabilization.” *Daedalus 134* (2005). http://nrs.harvard.edu/urn-3:HUL.InstRepos:342594.

Schneider, Jacquelyn G. “Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy.” *Lawfare* (blog). May 10, 2019. https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

Sherman, Justin. “Giant Report Lays Anvil on UC Cyber Policy.” *WIRED.com.* March 11, 2020. https://www.wired.com/story/opinion-giant-report-lays-anvil-on-us-cyber-policy/.

Smeets, Max. "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection." *Intelligence and National Security Vol. 35* (February 11, 2020). https://doi.org/10.1080/02684527.2020.1729316.

Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" *Lawfare (blog).* July 4, 2017. https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

Taddeo, Mariarosaria. "Norms and Strategies for Stability in Cyberspace." *ISPI – Report: The Global Race for Technological Superiority: Discover the Security Implications* (April 25, 2020). https://ssrn.com/abstract=3585082 or http://dx.doi .org/10.2139/ssrn.3585082.

Theohary, Catherine A. *Defense Primer: Cyberspace Operations.* CRS Report for Congress IF10537. Washington DC: Congressional Research Service, December 15, 2020. https://fas.org/sgp/crs/natsec/IF10537.pdf.

Tikk, Eneken, and Mika Kerttunen. "Parabasis: Cyber-Diplomacy in Stalemate." *Norwegian Institute of International Affairs* (2018). http://hdl.handle.net/11250/2569401.

U.S. Congress. House. Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities. *Statement of General Paul M. Nakasone, Commander, United States Cyberspace Command*. 116th Cong., March 4, 2020. https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.

U.S. Congress. Senate. Committee on Intelligence. *Hearing on Foreign Influence Operations and their Use of Social Media Platforms*. 116th Cong., September 5, 2018. *Political Transcript Wire.com.* Sep 05, 2018. https://search-proquest-com.lomc.idm.oclc.org/wire-feeds/senate-intelligence-committee-full-hearing-on/docview/2099599618/se-2?accountid=14746.

U.S. Congress. *National Defense Authorization Act for Fiscal Year 2020*, 116th Cong., Congressional Record (December 15, 2019), S 1790. https://www.congress.gov/.

U.S. Cyber Command. *US Cyber Command Vision: Achieve and Maintain Cyberspace Superiority* (April 20, 2018). https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

U.S. Cyberspace Solarium Commission Report. March 2020. https://www.solarium.gov/report.

U.S. Department of Defense. *Deterrence Operations Joint Operating Concept* (Version 2.0. Washington, DC, December 2006). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337.

U.S. Department of Defense. "Strategies for Operating in Cyberspace." Washington, DC, July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

U.S. Department of Defense. "Strategies for Operating in the Information Environment." Washington, DC, June 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

U.S. Department of Defense. *Summary of the 2018 Department of Defense Cyber Strategy* (Washington, DC, 2018). https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

U.S. Department of Defense. *Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge* (Washington, DC, 2018). https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

U.S. Department of Justice. *Report of the Attorney General's Cyber Digital Task Force* (July 2, 2018). https://www.justice.gov/ag/page/file/1076696/download.

U.S. Executive Office of the President, Council of Economic Advisors. "The Cost of Malicious Cyber Activity for the U.S. Economy." February 2018. https://www.hsdl.org/?view&did=808776.

U.S. Executive Office of the President. "Cyberspace Policy Review." April 3, 2014. https://www.nationalcyberwatch.org/resource/cyberspace-policy-review-assuring-a-trusted-and-resilient-information-and-communications-infrastructure-2/.

U.S. Executive Office of the President. *International Strategy for Cyberspace*. Washington, DC, May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

U.S. Executive Office of the President. *National Cyber Strategy of the United States of America*. Washington, DC, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

U.S. Office of the Press Secretary of the White House. "Fact Sheet: President Xi Jingping's State Visit to the United States." *The Obama White House Archives*. September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

U.S. Secretary of State Policy Planning Staff. *Elements of the China Challenge November 2020* (Washington, DC, 2020). Accessed December 1, 2020. https://www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf.

Valeriano, Brandon and Benjamin Jensen. “The Myth of the Cyber Offense: The Case for Restraint.” *CATO Institute Policy Analysis No. 862* (January 15, 2019). https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.

Weber, Rick. "DoD'S ‘Defend Forward’ Cyber Strategy Prompts Lively Debate by ABA.” *Inside the Pentagon's Inside the Army 31, No. 46* (November 18, 2019). https://search-proquest-com.lomc.idm.oclc.org/trade-journals/dods-defend-forward-cyber-strategy-prompts-lively/docview/2315038968/se-2?accountid=14746.

White House. *National Security Strategy February 2015*. Washington, DC, 2015. https://nssarchive.us/wp-content/uploads/2020/04/2015.pdf.

White House. *National Security Strategy of the United States of America December 2017*. Washington, DC, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

White House, Office of Trade and Manufacturing Policy. *How China’s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World June 2018* (Washington, DC, 2018). Accessed December 1, 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

Work, JD. “Insecurity, Capabilities Acquisition, and Conflict.” Class lecture. Cyber Operations, Intelligence and Conflict, Marine Corps University, Quantico, VA January 15, 2021.

Xuetong, Yan. “Bipolar Rivalry in the Early Digital Age.” *The Chinese Journal of International Politics*. June 2020. Accessed December 1, 2020. https://academic.oup.com/cjip/article/13/3/313/5854839.

Zheng, Denise E. “Critical Questions: 2015 DOD Cyber Strategy.” *Center for Strategic & International Studies* (website). April 24, 2015. https://www.csis.org/analysis/2015-dod-cyber-strategy.