



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**EFFECTS OF DEFEND FORWARD ON SECURITY,
STABILITY, AND U.S. INTERESTS IN THE
CYBERSPACE DOMAIN**

by

Zachary A. Poindexter

June 2022

Thesis Advisor:
Second Reader:

Wade L. Huntley
Michael Senft

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2022	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE EFFECTS OF DEFEND FORWARD ON SECURITY, STABILITY, AND U.S. INTERESTS IN THE CYBERSPACE DOMAIN			5. FUNDING NUMBERS	
6. AUTHOR(S) Zachary A. Poindexter				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The defend forward cyber defense strategy is predicated on the notion of persistent engagement with adversaries in gray and red network space, to cause friction for adversaries before they can carry out malicious activity in U.S. network space. The U.S. Cyber Defense Strategy seeks to overmatch adversaries and cause friction by actively engaging adversaries outside of U.S. network space, albeit below the threshold of armed conflict. This strategy is designed to advance the security of U.S. national interests in the cyberspace domain. U.S. security strategies may have varying effects on stability in specific domains and in overall international relations. Defend forward is often criticized for being destabilizing in the cyberspace domain, and as such, security gains from defend forward are potentially outweighed by negative effects of a further destabilized domain. This thesis answers the following questions: What is the impact of defend forward on the security of U.S. interests and overall stability in the cyberspace domain? The thesis seeks to separate the effects that defend forward has on security and stability in order to understand how, and to what extent, the strategy impacts both. This ultimately enables a determination of the immediate and long-term efficacy of defend forward and the role stability has in relation to the security of U.S. interests in the cyberspace domain.				
14. SUBJECT TERMS defend forward, persistent engagement, DCO, defensive cyber operations, cyberspace domain, stability, cybersecurity, cyber policy, USCYBERCOM, cyber command, deterrence, cyber, destabilization			15. NUMBER OF PAGES 85	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**EFFECTS OF DEFEND FORWARD ON SECURITY, STABILITY, AND U.S.
INTERESTS IN THE CYBERSPACE DOMAIN**

Zachary A. Poindexter
Lieutenant, United States Navy
BA, The University of Texas at Austin, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
June 2022**

Approved by: Wade L. Huntley
Advisor

Michael Senft
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The defend forward cyber defense strategy is predicated on the notion of persistent engagement with adversaries in gray and red network space, to cause friction for adversaries before they can carry out malicious activity in U.S. network space. The U.S. Cyber Defense Strategy seeks to overmatch adversaries and cause friction by actively engaging adversaries outside of U.S. network space, albeit below the threshold of armed conflict. This strategy is designed to advance the security of U.S. national interests in the cyberspace domain.

U.S. security strategies may have varying effects on stability in specific domains and in overall international relations. Defend forward is often criticized for being destabilizing in the cyberspace domain, and as such, security gains from defend forward are potentially outweighed by negative effects of a further destabilized domain.

This thesis answers the following questions: What is the impact of defend forward on the security of U.S. interests and overall stability in the cyberspace domain? The thesis seeks to separate the effects that defend forward has on security and stability in order to understand how, and to what extent, the strategy impacts both. This ultimately enables a determination of the immediate and long-term efficacy of defend forward and the role stability has in relation to the security of U.S. interests in the cyberspace domain.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	PERSISTENT ENGAGEMENT IN THE CYBERSPACE DOMAIN	1
A.	THE RELATIONSHIP BETWEEN SECURITY AND STABILIZATION AS A RESULT OF DEFEND FORWARD	2
B.	CYBERSPACE AND PERSISTENT ENGAGEMENT: A CRITICAL DOMAIN AND A NEW WAY FORWARD	4
C.	LITERATURE REVIEW—DEFEND FORWARD: SECURITY OR DESTABILIZATION?	6
1.	Evolution and Limitations of a Cyber Deterrence Strategy	6
2.	A Paradigm Shift.....	8
3.	Critiques of Persistent Engagement	10
4.	Questions of Cyberspace Stability	13
5.	The Concept of Stability in Cyberspace	15
II.	IMMEDIATE EFFECTS ON SECURITY AND STABILITY IN THE CYBERSPACE DOMAIN	19
A.	INITIAL EFFECT ON THE SECURITY OF U.S. INTERESTS IN THE CYBERSPACE DOMAIN	19
1.	Methodology	19
2.	Results	21
3.	Conclusion	25
B.	IMMEDIATE EFFECTS ON STABILITY	26
1.	Tangible Indicators of Stability Criteria Being Met.....	26
2.	Does Defend Forward Impact the Criteria for Stability?.....	30
3.	Conclusion	36
C.	CONCLUSION	37
III.	LONG-TERM EFFECTS ON CYBERSECURITY AND CYBERSPACE DOMAIN STABILITY.....	39
A.	SECURITY IN THE LONG-TERM.....	39
B.	STABILITY IN THE LONG-TERM.....	41
1.	Stabilization Through Cooperative Norms	42
2.	Defend Forward and Stabilizing Norms	44
3.	Defend Forward, Stability, and Unique Cyber Features	47
4.	Conclusion	49
C.	CONCLUSION	50
IV.	OVERALL EFFECTS OF DEFEND FORWARD.....	53

A.	DEFEND FORWARD AND THE SECURITY OF U.S. INTERESTS IN THE CYBERSPACE DOMAIN	54
B.	DEFEND FORWARD AND THE STABILITY OF THE CYBERSPACE DOMAIN	56
C.	THE DEGREE TO WHICH PROMOTING STABILITY SUPPORTS U.S. INTERESTS IN THE CYBERSPACE DOMAIN	58
D.	RESEARCH LIMITATIONS AND FUTURE WORK	60
1.	Research Limitations	60
2.	Future Work.....	62
LIST OF REFERENCES		65
INITIAL DISTRIBUTION LIST		71

LIST OF FIGURES

Figure 1.	Number of State Sponsored Cyber Incidents Perpetrated Against U.S. Interests	22
Figure 2.	Number of Cyber Incidents Severity by 4-Year Group	24
Figure 3.	Percent of Cyber Incidents Severity by 4-Year Group	24

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CFR	Council on Foreign Relations
DCO	Defensive Cyberspace Operation
DOD	Department of Defense
DODIN	Department of Defense Information Network
DDOS	Distributed Denial of Service
GCSC	Global Commission on the Stability of Cyberspace
ICANN	Internet Corporation for Assigned Names and Numbers
OPM	Office of Personnel Management
NSA	National Security Agency
US	United States
USCYBERCOM	United States Cyber Command

THIS PAGE INTENTIONALLY LEFT BLANK

I. PERSISTENT ENGAGEMENT IN THE CYBERSPACE DOMAIN

United States Cyber Command's (USCYBERCOM) mission is to "defend and advance U.S. national interests" in the cyberspace domain.¹ As the cyberspace domain is a nascent and nontraditional domain of war, the ways and means to achieve this defense have evolved significantly since USCYBERCOM's founding in 2009. With this evolution, understanding the effects of USCYBERCOM's strategy is critically important.

Furthermore, as the cyberspace domain is rapidly evolving with advances in technology and capability, stability is often heralded as being a desired end state for the stakeholders of the domain. In recent years, USCYBERCOM strategy has embraced a "defend forward" posture informed by recognition that "persistent engagement" defines the domain. Critics of this USCYBERCOM strategy often argue that destabilizing effects of the strategy can ultimately counteract any gains in security, based on a near ubiquitous understanding that a correlation between the security of United States (U.S.) interests and stability of the cyberspace domain exists. This coupling of security and stability forms the foundation of much of the criticism surrounding USCYBERCOM's defensive strategy. However, that coupling hampers analysis of the ultimate effects of the strategy on security and stability as distinct outcomes.

The core purpose of this thesis is to evaluate the separate impacts of the current USCYBERCOM strategy of "Defend Forward" on U.S. security interests and on overall stability in cyberspace. Analyzing each effect separately allows for greater understanding of the impact of the strategy on each distinct outcome, while at the same time illuminating the actual relationship between security and stability in the cyberspace domain.

¹ "Our Mission and Vision," U.S. Cyber Command, accessed April 30, 2022, <https://www.cybercom.mil/About/Mission-and-Vision/>.

A. THE RELATIONSHIP BETWEEN SECURITY AND STABILIZATION AS A RESULT OF DEFEND FORWARD

The 2018 USCYBERCOM Vision outlined a shift in strategy to “influence and shape adversary behavior through persistent, integrated operations.”² This was a pivot away from a purely deterrent-based cyber defense strategy and was coined “Defend Forward.” The Defend Forward cyber strategy is predicated on the notion that persistent engagement with adversaries in gray and red network space will cause friction for adversaries before they can carry out malicious activity in U.S. network space. This friction in turn will deincestivize attack U.S. interests in the cyberspace domain. The strategy seeks to overmatch adversaries and cause friction by actively engaging adversaries outside of U.S. network space, albeit below the threshold of armed conflict. This strategy is designed to advance U.S. national interests, both in cyberspace and more broadly.

However, critics of Defend Forward contend that the strategy could be destabilizing in the cyberspace domain, eroding the formation and adoption of cooperative norms of behavior.³ Stability in the cyberspace domain is an evolving concept, but is generally built from traditional concepts in international relations theory. Stability can be defined as the condition in which there is little risk of disputes escalating into offensive actions and the status quo is not at risk of changing. Stability can be logically viewed as a product of the international system and the behavior of the stakeholders.⁴ In the Cold War, the system was a balance of power in a bipolar system between the United States and the Soviet Union. This created an arguably stable environment in which both parties agreed on implicit rules for maintaining stability for fear of mutual destruction, thus violent change to the system did not occur.⁵ Following the collapse of the Soviet Union in the 1990s, the world

² U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, (Fort Meade MD, U.S. Cyber Command, 2018), <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>, 2.

³ Jason Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” *Journal of Cybersecurity* 5, no. 1 (January 2019): 1–15, <https://doi.org/10.1093/cybsec/tyz008>, 8.

⁴ John Lewis Gaddis, “The Long Peace: Elements of Stability in the Postwar International System,” *International Security* 10, no. 4 (1986): 99–142, <https://doi.org/10.2307/2538951>, 104.

⁵ Gaddis, 132.

experienced a system of unipolar hegemony under the United States.⁶ Theorists on both sides argued the stability or instability of this system, with proponents arguing that change was unlikely due to the “quantitative and qualitative material advantages” of the United States.⁷ Opponents argued that a unipolar hegemon would prompt other stakeholders to rise and create a bipolar or multipolar balance of power again.⁸ There is much disagreement on the nature and conditions of stability, but it is generally viewed as to U.S. complimentary to U.S. interests and lasting peace.

There are multiple theories of how stability can be achieved. The liberal view is that adoption of cooperative norms, which are mutually beneficial to the stakeholders, creates an equilibrium of stability in which breaking the norms would not benefit offender, and thus stability is encouraged. This contrasts with a realist view that norms are a product of a stable international system, in which nations find balance through seeking their own self-interest and security.⁹ Recent works propose that emerging technology, or in this case the cyberspace domain, will not change the fundamental nature of stability as technology can change the behavior, but not necessarily the systems in which they can be applied.¹⁰ However, pursuing stability in the cyberspace domain may not produce the best outcome to protect and further U.S. interests. The cyberspace domain is inherently unstable in its current state. It is often argued that the domain is immature, the uses of the domain are evolving rapidly, trust is elusive, and there are no agreed upon norms of behavior.¹¹ The prospect of exacerbating this instability in pursuit of security deserves serious attention.

⁶ William C. Wohlforth, “The Stability of a Unipolar World,” *International Security* 24, no. 1 (1999): 5–41, 23.

⁷ Wohlforth, 17.

⁸ Wohlforth, 6.

⁹ Scott Romaniak, and Francis Grice, “Norms, Norm Violations, and IR Theory,” *E-International Relations* (blog), November 15, 2018, <https://www.e-ir.info/2018/11/15/norms-norm-violations-and-ir-theory/>.

¹⁰ Todd S. Sechser, Neil Narang, and Caitlin Talmadge, “Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War,” *Journal of Strategic Studies* 42, no. 6 (2019): 727–35, <https://doi.org/10.1080/01402390.2019.1626725>, 729.

¹¹ Mark Raymond, “Confronting the Ubiquity of Norms in Cyberspace and Cyber Governance,” *Lawfare*(blog), March 12, 2020, <https://www.lawfareblog.com/confronting-ubiquity-norms-cyberspace-and-cyber-governance>.

While instability in a domain connotes negative implications, stability by its nature denies opportunity to change. Instability can offer opportunities to better one's posture and influence, especially in a domain that is inherently unstable. For this reason, U.S. national interests are not always served best strictly seeking a stable environment, and stability often is not the primary objective of U.S. security policies. Thus, if Defend Forward is inherently destabilizing, or inherently prevents stabilization, it does not necessarily imply that U.S. cyber security, and U.S. national interests more broadly, will be degraded. A destabilized domain could potentially favor the current U.S. positioning in the cyberspace domain and allow for greater security of U.S. interests in cyberspace as well as in the physical world.

Unlinking the automatic association of stability and the security of U.S. interests enables this thesis to provide a fuller evaluation of the efficacy of the Defend Forward strategy for U.S. objectives in cyberspace. This evaluation considers not only how and in what ways Defend Forward may affect the stability of the cyberspace domain, but separately how the strategy will affect the security of U.S. interests. The thesis assesses the potential effectiveness of this strategy by analyzing the immediate and long-term effects of Defend Forward on security of U.S. interests and the stability of the cyberspace domain. In so doing, this thesis identifies challenges that may arise in trying to maximize security while also considering the effects on the stability of the cyberspace domain.

B. CYBERSPACE AND PERSISTENT ENGAGEMENT: A CRITICAL DOMAIN AND A NEW WAY FORWARD

The cyberspace domain is the newest, most interconnected, yet most ill-defined and misunderstood domain of war today. Simultaneously, cyberspace is a critical domain for U.S. national interests. In today's world, cyberspace is key to advancing economic interests, security, and influence. Nearly all the world's major industries rely on networked resources for production, investment, and dissemination of goods. Defense strategies rely on the safe and secure sharing, disseminating, and protection of information. And global influence is spread via unparalleled interconnected means of communications in the cyberspace domain. The United States has a vested interest in protecting, supporting, and expanding these national interests for the American People, and thus being able to secure

cyberspace as a domain, and defend these national interests in the cyberspace domain is vital.

As vital as the cyberspace domain is to U.S. national interests, many uncertainties exist when it comes to understanding cyberspace. Its multilayered and seemingly abstruse nature often requires description in terms of analogy and multi-layered models. These uncertainties make effective defense in this domain difficult to plan, execute, and articulate. Additionally, the immediate and long-term effects of any defense strategy are difficult to predict, as the complex interactions of the cyberspace domain and the world at large are continuing to expand, develop, and evolve.

Prior to 2018, cyber defense under USCYBERCOM was conducted with a deterrence-based mindset. Early defense revolved around the idea of providing strong information security on the networks, and response actions against operators involved in any malicious activity carried out against the Department of Defense Information Network (DODIN), to deter attacks from occurring. As General Paul Nakasone, the Commander of USCYBERCOM points out, this was done in anticipation of threats against U.S. interests above the threshold of armed conflict, and in response to attacks against U.S. forces in Iraq and Afghanistan.¹²

But within a matter of years, this strategy proved ineffective against many attacks that occurred below the threshold of armed conflict but had strategic level effects.¹³ The fear of vertical escalation prevented the DOD from taking response actions, leading to frustration from policy makers, and as USCYBERCOM Strategist Emily Goldman describes, the response actions that did occur seemed infrequent and sporadic, and thus deterrence appeared ineffective.¹⁴

¹² Paul Nakasone, "Introduction: A Cyber Force For Persistent Operations," In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner (Newport RI: U.S. Naval War College Press, 2020), 1–8, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>, 3.

¹³ Nakasone, 3.

¹⁴ Emily Goldman, "The Cyber Paradigm Shift," In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner (Newport RI: U.S. Naval War College Press, 2020), 31–46, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>, 38.

The shift to a persistent engagement-based strategy reflected the conclusion that the previous strategy was not effectively addressing the evolving threats in the cyberspace domain, and that these threats could in turn have strategic implications.¹⁵ This radical strategic shift was a departure from existing paradigms in security strategy, in part because persistent engagement does not fit cleanly into traditional definitions of offense and defense.¹⁶ As such the effects of this new strategy are still unclear, and thus research into potential effects of this strategy are significant as the DOD has invested and adopted this new strategy to counter threats in cyberspace.

C. LITERATURE REVIEW—DEFEND FORWARD: SECURITY OR DESTABILIZATION?

1. Evolution and Limitations of a Cyber Deterrence Strategy

USCYBERCOM was formed in 2010 as a response to disruption and exploitation attacks against DOD information systems and U.S. critical infrastructure. Its mission focused on “checking the capability development of ... competitors, [and] supporting ongoing operations in Iraq and Afghanistan.”¹⁷ USCYBERCOM’s mission was buttressed by the *2011 International Strategy for Cyberspace* and the *2015 DOD Cyber Strategy* which outlined the U.S. cyber strategy in terms of deterrence. The 2015 DOD Cyber Strategy outlines that DOD “if directed by the President or the Secretary of Defense, ... may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace.”¹⁸ Attacks of “significant consequence” could prompt a response action if and only if they were green lit by the President or the Secretary of Defense.¹⁹

¹⁵ Nakasone, “Introduction: A Cyber Force For Persistent Operations,” 3.

¹⁶ Goldman, “The Cyber Paradigm Shift,” 38.

¹⁷ Nakasone, “Introduction: A Cyber Force For Persistent Operations,” 3.

¹⁸ U.S. Department of Defense, *The DOD Cyber Strategy* (Washington, DC: Department of Defense, 2015), <https://www.hsdl.org/?abstract&did=764848>, 5.

¹⁹ U.S. Department of Defense, 5.

This strategy reflects deterrence methodology as developed in the Cold War, in what Emily Goldman described as a continuation of the “deterrence paradigm.”²⁰ Significant attacks taken against the U.S. or U.S. interests are met with a response attack, authorized at the highest level, thus coercing the adversary to not act. This strategy worked well in the Cold War nuclear context, when neither the U.S. nor Soviet Union were willing to use nuclear weapons for fear of a response in kind. As Emily Goldman describes: the leaders who cut their teeth in a Cold War context, applied the strategies and policies they saw effective against the Soviet Union in the new Cyberspace domain.²¹ Deterrence strategy was applied to the cyberspace domain to counter the large-scale attacks that would be above the level of armed conflict, however as the cyberspace domain continued to evolve these types of attacks no longer were the only serious threat the U.S. faced.

As early as 2012–2013, the world began tracking attacks in the cyberspace domain that remained below the level of armed conflict, but had strategic implications. General Nakasone highlighted the Iranian Denial of Service attacks against financial institutions in 2012–2013, the North Korean hack of Sony Pictures entertainment in 2014, and China’s disruption of GitHub and the theft of information from the U.S. Office of Personal Management in 2015.²² Emily Goldman described these events as “anomalies” in the deterrence paradigm, as the deterrence strategy was ineffective against them.²³ The U.S. defense strategy in cyberspace was not designed to counter these new types of threats. Because these attacks were not considered armed conflict, the political risk of escalation was high if a response action was taken, which in turn led to an unwillingness to act at the highest level. Attackers could assess that this type of response was unlikely, and thus as Michael Fischerkeller and Richard Harknett describe, there was no coercive act or tacit

²⁰ Goldman, “The Cyber Paradigm Shift,” 33.

²¹ Goldman, 34.

²² Nakasone, “Introduction: A Cyber Force for Persistent Operations,” 3.

²³ Goldman, “The Cyber Paradigm Shift,” 34.

bargaining at play to create stability and deter attacks.²⁴ This is the scenario that General Nakasone faced, and what prompted a shift away from a solely deterrence-based strategy.

2. A Paradigm Shift

In 2018, General Nakasone announced a pivot from the deterrence and response action model of Defensive Cyberspace Operations (DCO) in order to provide a proactive defense: to “defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage.”²⁵ This strategic shift, coincided with Congress “clarify[ing] the statutory authority for military cyber operations to enable Cyber Command to conduct traditional military activities in addition to the mostly preparatory operations to which it had been limited previously,” and a new U.S. National Cyber Strategy, which eased authorization restrictions on cyber operations, and gave commanders more flexibility to act in the cyberspace domain.²⁶

As Emily Goldman describes, this represents a paradigm shift away from deterrence.²⁷ As more and more anomalous attacks occurred, which the existing deterrence strategy could not stop, General Nakasone championed a new way forward to persistently engage with adversaries to create friction and provide a more holistic defense.²⁸ Fischerkeller, Harknett, and Goldman describe the new persistent engagement paradigm as recognizing attacks that occur below the level of armed conflict not as anomalies, but rather

²⁴ Michael P. Fischerkeller and Richard Harknett, “Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace,” *Lawfare* (blog), November 9, 2018, <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>.

²⁵ U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, 2.

²⁶ U.S. Department of Defense, *National Cyber Strategy* (Washington, DC, Department of Defense, 2018), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>, 2; Paul Nakasone and Michael Sulmeyer, “How to Compete in Cyberspace,” *Foreign Affairs*, March 17, 2021, <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>.

²⁷ Goldman, “The Cyber Paradigm Shift,” 41.

²⁸ U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, 4.

as evidence of competitive activity in a domain wherein “agreement over the substantive character of acceptable and unacceptable behaviors . . . is currently immature.”²⁹

Proponents see Defend Forward as a better way to counter the ever-evolving threats to U.S. interests in the cyberspace domain, particularly as attacks below the threshold of armed conflict are becoming the “normal,” and which can cause strategic effects.³⁰ Max Smeets point out that the 2018 Vision accepts the notion that “activities in cyberspace that do not rise to the level of armed conflict may nevertheless have strategically significant effects”:³¹

The spread of technology and communications has enabled new means of influence and coercion. Adversaries continuously operate against us below the threshold of armed conflict. In this “new normal,” our adversaries are extending their influence without resorting to physical aggression. They provoke and intimidate our citizens and enterprises without fear of legal or military consequences. They understand the constraints under which the United States chooses to operate in cyberspace, including our traditionally high threshold for response to adversary activity. They use this insight to exploit our dependencies and vulnerabilities in cyberspace and use our systems, processes, and values against us to weaken our democratic institutions and gain economic, diplomatic, and military advantages.³²

Nakasone and proponents of the 2018 strategic shift recognize that these are the attacks that deterrence failed to address. This recognition “reflects the fact that one-off cyber operations are unlikely to defeat adversaries. Instead, U.S. forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time.”³³ For proponents, this is the *raison d’être* of the persistent engagement strategy.

²⁹ Goldman, “The Cyber Paradigm Shift,” 39.

³⁰ Michael Warner, “A Brief History of Cyber Conflict,” In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner (Newport RI: U.S. Naval War College Press, 2020), 13–31, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>, 17.

³¹ Max Smeets, “What Is Absent From the U.S. Cyber Command ‘Vision’,” *Lawfare*(blog), May 3, 2018, <https://www.lawfareblog.com/what-absent-us-cyber-command-vision>.

³² U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, 4.

³³ Nakasone and Sulmeyer, “How to Compete in Cyberspace.”

3. Critiques of Persistent Engagement

The notion of a new paradigm in the cyberspace domain, based on a persistent engagement model as the most effective means to defend Department of Defense (DOD) networks, critical infrastructure, and U.S. interests, is not universally accepted. At the heart of much of the criticism of persistent engagement is the idea that it is inherently destabilizing or, in the context of an already unstable domain, prevents stabilization. Moreover, the cyberspace domain is still novel enough that predictable outcomes of actions taken in the domain are difficult to calculate.

Jason Healey posits that persistent engagement provides many “opportunities for mistake, misperception, and miscalculation,” and that if “strategic stability” is the policy goal, a strategy of “stability-enhancement engagement” could be more effective than persistent engagement.³⁴ Healey assesses that while Defend Forward may create a more cohesive and encompassing defense strategy, the risks associated with it do not seem to be being adequately addressed by USCYBERCOM.³⁵ Specifically, he argues that USCYBERCOM is portraying Defend Forward, and persistent engagement, as the only strategy to achieve stability and superiority and thus security. It is notable here that Healey’s critique builds from two premises: that persistent engagement may be destabilizing, and that cyberspace stability is an intrinsic U.S. security interest. This thesis assesses both of those premises.

Healey also observes that USCYBERCOM is blinding the U.S. to alternatives in order to free its hands to act, and that this is a slippery slope to overreaction. For comparison, Healey points to the counterproductive nature of using overwhelming firepower being “fatal” to a counter insurgency campaign.³⁶ For example, the Army may feel it has an imperative to use overwhelming force to achieve its objective, but in reality, this makes the objective impossible to obtain in an insurgency environment. The evaluation in this thesis will shed light on how aptly such analogies describe cyberspace conflict.

³⁴ Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” 12.

³⁵ Healey, 6.

³⁶ Healey, 6.

Other critics contend that Defend Forward is risking the destabilization of relationships with allies and partners. Max Smeets points out that by being engaged with adversaries in allies' networks, the strategy "creates friction by allies undermining trust."³⁷ Additionally, Defend Forward operations could undermine allied intelligence operations in the cyberspace domain, creating more friendly friction, which could be exploited by potential adversaries.³⁸ Smeets emphasizes that if allied or partner nations conduct their own persistent engagement style operations, not in tandem with the U.S., this could cause even more friendly friction and destabilization of relations.³⁹

Arguments have also been made that persistent engagement may lead to "turf battles" withing U.S. agencies, as intelligence services have long been present on networks, siphoning data and collecting information. As Max Smeets points out, there is a difference between intelligence operations and military operations. Not only could military operations in foreign networks spark more reaction from foreign nations than intelligence collection, the risk of "turf battles" between USCYBERCOM and the National Security Agency (NSA), both of which may want access to the same adversary networks but with much different intents, is likely.⁴⁰

Joshua Rovner argues that competition in cyberspace presents an intelligence contest vice a military contest, in that it is concerned with procuring, controlling, and securing information. Military contests on the other hand employ traditional strategic theory to employ physical strength. He argues that applying strategic theory, designed around military contests, does not necessarily apply in the cyberspace domain where strength is not measured in physical prowess, and convert action is routine.⁴¹ By this logic notions of offense, defense, and deterrence do not generally apply, and viewing cyberspace

³⁷ Max Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 35, no. 3 (April 15, 2020): 444–53. <https://doi.org/10.1080/02684527.2020.1729316>, 445.

³⁸ Smeets, 450.

³⁹ Smeets, 445.

⁴⁰ Smeets, 446.

⁴¹ Joshua Rovner, "Cyber War as an Intelligence Contest," War on the Rocks, September 16, 2019, <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/>.

through the lens of a military domain is unproductive. The very disagreement over the nature of contests in the cyberspace domain adds to the instability of the domain. An equilibrium is elusive if one cannot identify the nature of the mechanisms influencing the domain.

James Miller and Neil Pollard focus their critique on Fischerkeller and Harknett's notion of an "agreed competition" based in tacit bargaining in the cyberspace domain.⁴² Fischerkeller and Harknett argue that by being more active in the domain, and persistently engaging with adversaries, the U.S. will lead the way in the development of norms in cyberspace, and tacit bargaining will define the guardrails of expectable and proportional action.⁴³ Miller and Pollard point out that this may be a naïve view, as one cannot look at the cyberspace domain in isolation. The cyberspace domain is interconnected to the physical domains, and conflict or activity that occurs in cyberspace can ricochet and expand out into other domains and "other dimensions of international competition," making the notion of a stabilizing "agreed competition" in cyberspace flawed.⁴⁴ It is notable here that, like Healy, Miller and Pollard's critique flows from the premises that persistent engagement may be destabilizing and that cyberspace stability is an intrinsic U.S. security interest.

Miller and Pollard advocate that the risk of escalation must be met with deterrence and not persistent engagement alone. They point to the examples of intellectual property theft from Chinese "cyber-related activity," and assert that the U.S. cannot afford to tolerate these actions as "inevitable" and thus they must be deterred.⁴⁵ Miller and Pollard argue that deterrence is necessary below the level of armed conflict, and serves as an effective means not only to prevent attack and escalation, but also by influencing adversary behavior, as "strong cyber responses (which carry risk of vertical escalation) and noncyber responses

⁴² James Miller and Neal Pollard, "Persistent Engagement, Agreed Competition and Deterrence in Cyberspace," *Lawfare* (blog), April 30, 2019, <https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace>.

⁴³ Fischerkeller and Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace."

⁴⁴ Miller and Pollard, "Persistent Engagement, Agreed Competition and Deterrence in Cyberspace."

⁴⁵ Miller and Pollard.

(which constitute horizontal escalation) will affect the other side's perception of costs and risks."⁴⁶ Here, Miller and Pollard seem to be resisting the "paradigm shift" that Goldman and others contend is essential to diagnosing the nature of today's cyber threats to U.S. security.

4. Questions of Cyberspace Stability

While critiques of persistent engagement and Defend Forward push for greater understanding, clarification, and adjustment, there is wide agreement that the pre-2018 strategy was outdated and change was necessary. Analysts on both sides of this debate view USCYBERCOM being more active and proactive in the cyberspace domain as a positive change for increasing security. Viewpoints diverge mainly on the outstanding question of what the overall effects of persistent engagement will be, particularly for cyberspace stability. Smeets and Lin point out the need for research into how Defend Forward will "play out."⁴⁷ Healey calls for research on the long-term effects of a persistent engagement, particularly the effects of making strategic decisions to achieve an underlying end of stability versus a more immediate end of security.⁴⁸ Both of these calls for research highlight the vast unknowns of operational and strategic effects when it comes to the cyberspace domain.

The notion that lasting security is correlated with, if not dependent on stability is a common understanding. In the twentieth century, one can see this best in Cold War detente policy. In the late 1960s and early 1970s, the Nixon and Brezhnev administrations sought to relax their strained relations and thus stabilize great power and international relations. This in turn would soften the great power competition and lead to greater security for both sides.⁴⁹ Similar strategies can be seen in the Obama administration relaxing relations with

⁴⁶ Miller and Pollard.

⁴⁷ Max Smeets and Herb Lin, "An Outcome Based Analysis of U.S. U.S. Cyber Strategy of Persistence & Defend Forward," *Lawfare* (blog), November 28, 2018, <https://www.lawfareblog.com/>.

⁴⁸ Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," 12.

⁴⁹ Stephen Kieninger, "A Preponderance of Stability: Henry Kissinger's Concern over the Dynamics of Ostpolitik," *The Journal of Transatlantic Studies* 17, no. 1 (March 2019): 42–60, <http://dx.doi.org/10.1057/s42738-019-00003-3>, 45.

the Castro regime in Cuba, and the Trump administration holding presidential summits with Kim Jong Un of North Korea.⁵⁰ This strategy of seeking security through stability is based on the idea that instability intrinsically leads insecurity. In a destabilized environment, threats or attacks can come from any quarter and can use any conceivable vector.

It is important to note that the security-enhancing stability entailed in these examples requires minimum levels of adversarial engagement and cooperation. In US-Soviet détente, for example, formal arms control treaties provided the cornerstones for mutual expectations of more stabilizing behavior. This is why, for both supporters and critics of persistent engagement, cyberspace stability entails some level of development of norms of behavior mutually supported by all principal actors.⁵¹

Thus, it appears that cyberspace stability hinges on some level of adversarial cooperation, even if only informal and implicit. This raises the question of whether the unique features of the cyberspace domain can support such a climate of behavior. The novel nature and unprecedented characteristics of the cyberspace domain make it difficult to generate satisfactory analogous behavioral patterns with traditional domains. As such, what is true for other domains may not in fact be true for the cyberspace domain.

For example, Healey contends that stability is desirable in the long term, and that for the U.S. to achieve stability, it must prioritize stability; security will flow from that.⁵² Millar and Pollard are concerned by the risk of vertical and horizontal escalation leading to instability, and thus preventing security.⁵³ These concerns are valid given comparisons to traditional domains, but cyberspace is its own beast. The unique characteristics of the

⁵⁰ Donald Trump, “Remarks by President Trump and Chairman Kim Jong Un in a 1:1 Conversation,” U.S. U.S. Embassy & Consulate in Vietnam, February 28, 2019, <https://vn.usembassy.gov/20190227-remarks-president-trump-chairman-kim-11-conversation/>; Jenna Brayton, “The Seventh Summit of the Americas: The President’s Trip and a Historic Meeting,” [whitehouse.gov](https://obamawhitehouse.archives.gov/blog/2015/04/13/seventh-summit-americas-presidents-trip-and-historic-meeting), April 13, 2015, <https://obamawhitehouse.archives.gov/blog/2015/04/13/seventh-summit-americas-presidents-trip-and-historic-meeting>.

⁵¹ Fischerkeller and Harknett, “Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace.”

⁵² Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” 12.

⁵³ Miller and Pollard, “Persistent Engagement, Agreed Competition and Deterrence in Cyberspace.”

domain create a need to better understand the relationship of security and stability under these distinct characteristics, and specifically the nature of stability and security in a persistent engagement cyberspace paradigm. Without assuming that stability and security are complementary outcomes, one can more fully explore the effects of persistent engagement with a focus on identifying the tensions between these objectives, both in the short-run and in the long-run.

There is concern, even amongst the proponents of Defend Forward, that stability may be difficult to achieve with persistent engagement.⁵⁴ Thus there is utility in decoupling security from stability to examine the effectiveness of the Defend Forward in achieving its objective of security for U.S. interests in the cyberspace domain. By examining immediate and long-term effects of persistent engagement on security and stability separately, the questions of whether the U.S. can achieve a more secure environment for U.S. national interests, and whether stability is desirable for that end, can more explicitly be examined.

5. The Concept of Stability in Cyberspace

The concept and definition of stability in cyberspace is as dynamic as the domain. There is no uniform understanding of what stability looks like, let alone how one would achieve it. Inherent structural characteristics of the cyberspace domain also make stability an elusive goal. In international relations theory stability is a condition of equilibrium, where the status quo is not a risk of sudden or violent change.⁵⁵ More realist theoreticians see stability as a product of a balance of power and self-interest, where behavioral norms are a byproduct resulting from an existing balance.⁵⁶ Liberal theorists tend to view stability as a condition resulting from cooperative norms of behavior willingly adhered to by multi-stakeholders and based on mutually beneficial principles.⁵⁷

⁵⁴ Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” 12.

⁵⁵ Romaniak and Grice, “Norms, Norm Violations, and IR Theory.”

⁵⁶ Romaniak and Grice; Vaughn Shannon, “International Norms and Foreign Policy,” in *Oxford Research Encyclopedia of Politics*, Oxford University Press (Oxford: Oxford University Press, 2017), <https://doi.org/10.1093/acrefore/9780190228637.013.442>, 13

⁵⁷ Shannon, 13.

In cyberspace the waters get murkier. The cyberspace domain is constantly and rapidly evolving, so a condition in which a status quo is achieved, let alone maintained, is not necessarily feasible. As a result, there have been many attempts to define what a condition of stability in cyberspace may look like. These attempts redefine stability from a more general lack of risk of sudden change, to a definition of a most desired condition.

In 2014 the U.S. State Department published a framework to achieve their idea of stability in cyberspace. They defined stability as “an environment where all participants can positively and dependably enjoy its benefits, where there are incentives for cooperation and avoidance of conflict, and where disincentives for engaging in malicious cyber activity apply.”⁵⁸ The State Department proposed achieving this state through the development of cooperative norms of behavior. To create these norms, they proposed the U.S. work to establish bilateral cooperative agreements and then building these bilateral relations out to create multilateral agreements, eventually creating a critical mass of acceptance. They envisioned that the U.S. could lead by example to generate and promulgate norms to create guidelines for “responding to crimes, international rules of the road, information sharing, combating intellectual property theft, expanding education, and promoting attribution and prosecution of malicious actors.”⁵⁹ These norms in turn would generate the desired condition of stability.

While the U.S. State Department envisioned the U.S. taking the lead at creating norms to generate stability, this has not been the only approach in recent years. The Global Commission on the Stability of Cyberspace (GCSC), an organization initiated by the Hague Center for Strategic Studies and the EastWest Institute took on the challenge of defining stability in cyberspace, while fully articulating the ever-changing and evolving landscape of the cyberspace domain. They defined stability in cyberspace as a condition where “everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and

⁵⁸ International Security Advisory Board, *Report on A Framework for International Cyber Stability*, (Washington, DC, U.S. U.S. Dept of State, 2014), 3.

⁵⁹ International Security Advisory Board, 3.

where tensions are resolved in a non-escalatory manner.”⁶⁰ The Commission emphasized the need for “agile mechanisms” to adapt their norms to a constantly evolving domain. The norms they propose are grounded in principles of “responsibility, restraint, requirement to act, and a respect for human life.”⁶¹ By adhering to these principles, they asserted in 2019 and again in 2021 that norms can change and adapt, while still adding to their desired condition of stability.⁶² The commission defined their norms to be adopted by multistakeholders as:

1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.
2. State and non-state actors must not pursue, support, or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda, or plebiscites.
3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.
4. State and non-state actors should not commandeer the general public’s ICT resources for use as botnets or for similar purposes.
5. States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.
6. Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and
7. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.
8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.⁶³

⁶⁰ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, (New York NY, The Hague Centre for Strategic Studies, EastWest Institute, 2019), https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf, 13.

⁶¹ Global Commission on the Stability of Cyberspace, 18.

⁶² Alexander Klimburg, “New Conditions and Constellations in Cyber,” *Cyber Stability Paper Series* (The Hague: The Hague Centre for Strategic Studies, 2021), <https://hcss.nl/report/cyberstability-paper-series-new-conditions-and-constellations-in-cyber/>, 10.

⁶³ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 21.

The Commission arrived at their definition of Cyberstability from a bottom-up approach, in that they defined their norms, based on the principles they set forth, and extrapolated out to a desired end state. In 2021, Alexander Klimburg, the Director of the Commission, viewed their contribution to the development of the evolving definition of stability in cyberspace as the Group's most influential accomplishment.⁶⁴

The GCSC definition of stability illustrates a near utopian vision of what the cyberspace domain could be. This liberal theorist paradigm sees security in cyberspace as a product of the condition of stability. But this leads to the question of how feasible, or desirable, is a stable state in cyberspace as defined by the GCSC? Intrinsic characteristics of the cyberspace domain make stability incredibly elusive. Technology is constantly evolving, difficulty of attribution and secrecy make trust amongst stakeholders difficult, and disagreement over acceptable use of cyberspace by stakeholders all make stability a difficult end state to achieve.

This thesis evaluates how Defend Forward may affect the evolution of stability in cyberspace per the GCSC definition and the effects on security of U.S. interests. Security for U.S. interests in cyberspace is the goal of Defend Forward, and it may be possible despite a lack of stability in the domain.

⁶⁴ Klimburg, "New Conditions and Constellations in Cyber," 10.

II. IMMEDIATE EFFECTS ON SECURITY AND STABILITY IN THE CYBERSPACE DOMAIN

To assess the overall effects that Defend Forward has on the security of U.S. interests and the stability of the cyberspace domain, it becomes critical to first assess the immediate effects Defend Forward has had on both the security of U.S. interests, and the stability of the domain as defined by the GCSC. To assess the effects on the security of U.S. interests, research identified a data set of cyber incidents that occurred in the years before and after the strategic shift to Defend Forward in 2018. Section A reviews this data to assess any change in patterns which could point to an effect that Defend Forward had on security.

To measure any effects on stability, the analysis in this chapter develops four criteria from the definition of stability created by the GCSC in 2019. Section B utilizes these criteria to identify any positive move toward stability and conversely any distinct moves away from stability as a result of Defend Forward actions.⁶⁵ By assessing individual positive or negative movements toward meeting these criteria, and linking them to Defend Forward, the strategy can then be assessed as having a stabilizing or destabilizing effect on the cyberspace domain.

A. INITIAL EFFECT ON THE SECURITY OF U.S. INTERESTS IN THE CYBERSPACE DOMAIN

1. Methodology

To assess the effects of Defend Forward on the security of U.S. interests in the cyberspace domain, the data set of cyber incidents, which is maintained by the Council on Foreign Relations (CFR), was used. This database records publicly available information on all cyber incidents attributed to State actors. The database does not record incidents which were undertaken by criminal organizations or other non-state actors but is sufficient to illustrate overall trends in cyber incidents which targeted U.S. interests. The CFR database was filtered to only assess incidents in which the United States or U.S. interests

⁶⁵ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 13.

were the victim. The stated goal of Defend Forward is to increase the security of U.S. interests, therefore any effect on the security of U.S. interests should be examinable in this subset of incidents from the CFR database.

From this point the incidents were then combined into 4-year groupings to provide adequate differential variables in the data sets. The most recent year group was 2018–2021, encompassing the most recent data in the data base following the implementation of Defend Forward. The remaining year groups were 2014–2017, 2010–2013, and 2006–2009. In addition to simply counting the number of incidents in the years groups for a quantitative assessment, the severity of the incidents was assessed to provide a qualitative analysis. To identify the severity the scale adopted by the *Dyadic Cyber Incident and Dispute Data version 1.5 Codebook* was used. This project led by Professor Ryan Maness at the Naval Postgraduate School, categorizes State on State cyber incidents on a scale of one to ten, with ten being the most severe.

1. Probing/packet sniffing without kinetic cyber.
2. Harassment, propaganda, nuisance disruption.
3. Stealing targeted critical information
4. Widespread government, economic, military, or critical private sector network intrusion
5. Single critical network infiltration and physical attempted destruction
6. Single critical network infiltration and widespread destruction.
7. Minimal death as direct result of cyber incident.
8. Critical national economic disruption as a result of cyber incident.
9. Critical national infrastructure destruction as a result of cyber incident.
10. Massive death as a direct result of cyber incident.⁶⁶

This severity scale allowed for a uniform assessment of incidents to identify any patterns or shifts, specifically in relation the to Defend Forward. The number of incidents combined with the severity information were then used to assess any potential escalation in incidents, particularly in relation to 2018 when Defend Forward was implemented. In total 139 incidents were counted and assessed.

⁶⁶ Ryan Maness, Brandon Valeriano, and Brandon Jensen, “The Dyadic Cyber Incident and Dispute Data, Version 1.5,” the Naval Postgraduate School, Accessed April 6, 2022, <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.

2. Results

Through analysis of the number and severity of cyber incidents from 2006–2021, it is difficult to assess the effects Defend Forward has on the security of U.S. interests in the cyberspace domain. While the data showed an increase in the number of State-backed cyber incidents targeting U.S. interests, this increase cannot be definitively attributed to Defend Forward, as global trends of using the cyberspace domain as a vector of attack are increasing at a rapid rate.⁶⁷ There is also no data that suggests that the severity of cyber incidents is increasing, as the ratios of severity to total number of incidents has remained relatively constant. At minimum, this evidence suggests that Defend Forward is not any less effective than the pre-2018 Deterrence strategy, as the trend of increases in cyber incidents targeting the U.S. was present before the switch to Defend Forward.

a. Quantitative Assessment

An assessment of the number of cyber incidents from 2006–2021 revealed that in every 4-year grouping, the number of cyber incidents perpetrated by State actors against U.S. interests has increased. As shown in Figure 1, the number of incidents nearly doubled between 2010–2013 and 2014–2017, and then more than tripled between 2014–2017 and again in 2018–2021.

⁶⁷ “Tracking State-Sponsored Cyberattacks Around the World,” Council on Foreign Relations, Accessed April 10, 2022, <https://www.cfr.org/cyber-operations>.

Year	# of Incidents	4-Year Group Total
2021	28	85
2020	2	
2019	14	
2018	21	
2017	5	27
2016	5	
2015	7	
2014	10	
2013	2	14
2012	3	
2011	7	
2010	2	
2009	3	13
2008	4	
2007	3	
2006	3	

Figure 1. Number of State Sponsored Cyber Incidents Perpetrated Against U.S. Interests⁶⁸

The tripling of cyber incidents after 2017 correlates to the implementation of Defend Forward. On its face, this indicates that Defend Forward resulted in more cyber incidents, and thus a decrease in security. But of course, correlation does not prove causation. It is much more probable that the continued increase in incidents is evidence of the continued increase in number and volume of states using the cyberspace domain as a vector for attack, as that vector becomes more and more viable. Supporting this observation, this data set shows an increase in attacks between every 4-year group, and at an increasing rate.

Nevertheless, this data does not demonstrate that Defend Forward dramatically decreased the number of cyber incidents targeting U.S. interests. This could mean that Defend Forward is no better at providing security than the deterrence-based strategy that was in place before 2018. However, this determination is flawed as the increase in cyber

⁶⁸ Adapted from Council on Foreign Relations.

incidents may outweigh any security benefit from Defend Forward. In other words, Defend Forward may be better at preventing cyber incidents, and without this posture the increased rate of cyber incidents targeting the U.S. would have been even larger. This possibility is supported by multiple predictions of cybersecurity experts, who at the start of 2018, predicted large scale increases in the quantity and severity of cyber incidents, after years of an ineffective deterrence strategy from USCYBERCOM.⁶⁹ While the quantity of attacks did indeed increase, the severity of the attacks remained relatively constant.

b. Qualitative Assessment

After assessing the change in the number of cyber incidents in the four 4-year groups, the severity scale developed in the Maness codebook was applied to each incident with the intention of highlighting any patterns in the severity of State-backed cyber incidents targeting U.S. interests. The results of this application showed that 100 percent of the incidents from 2006–2021 that targeted U.S. interests fell within the range of 2–4 of the severity scale.

- 2—Harassment, propaganda, nuisance disruption Example - (Propagandist messages in Ukraine, Vandalism, DDoS in Georgia, Bronze Soldier dispute) Notes—Mainly vandalism or DDoS campaigns, this measure is coded when pockets of government or private networks are disrupted for periods of time and normal day to day online life is difficult, but recoverable.
- 3—Stealing targeted critical information Example - (Chinese targeted espionage, government-sanctioned cybercrime, Sony Hack) Notes - This involves the use of intruding upon a secure network and stealing sensitive or secret information. The theft of Lockheed Martin’s F-35 jet plans or the U.S. Department of Defense’s strategy in the Far East are examples. Or if the target was critical to national security or the objective of the attack had national security implications. The piggyback method is another example of this severity type. The United States’ NSA was able to piggyback on China’s Byzantine Series undetected and spy on the targets that the original espionage was spying upon.

⁶⁹ Alison DeNisco Rayome, “Forrester’s Top 6 Cybersecurity Predictions for 2018,” TechRepublic, November 7, 2017, <https://www.techrepublic.com/article/forresters-top-6-cybersecurity-predictions-for-2018/>; Paul Rosenzweig, “Cybersecurity Predictions for 2018,” *Lawfare* (blog), January 2, 2018, <https://www.lawfareblog.com/cybersecurity-predictions-2018>.

- 4—Widespread government, economic, military, or critical private sector network intrusion Example - (U.S. OPM hack, DOD employee records stolen, IRS hack) Notes –Phishing and intrusion espionage campaigns that successfully steal large troves of critical information, such as the OPM hack.⁷⁰

In every 4-year group incidents with a severity of 3 were the most common. This did not shift in the final 4-year group of the dataset, however in the final dataset, the percentage of severity level 3 incidents was significantly higher, than in previous year groups. This increase in Level 3 incidents was accompanied by a decrease in the percentage of Level 2 and Level 4 incidents, as compared to year groups before 2018.

4-Year Groups	Total Incidents	# Severity 4	# Severity 3	# Severity 2
2018-2021	85	16	62	7
2014-2017	27	8	14	5
2010-2013	14	2	8	4
2006-2009	13	3	8	2

Figure 2. Number of Cyber Incidents Severity by 4-Year Group⁷¹

4-Year Groups	% Severity 4	% Severity 3	% Severity 2
2018-2021	19%	73%	8%
2014-2017	30%	52%	19%
2010-2013	14%	57%	29%
2006-2009	23%	62%	15%

Figure 3. Percent of Cyber Incidents Severity by 4-Year Group⁷²

As with the quantitative assessment, this shift while correlated to the implementation of Defend Forward, does not imply causation from Defend Forward. Global trends of increased use of the cyberspace domain by State sponsored actors to

⁷⁰ Maness, Valeriano, and Jensen, “The Dyadic Cyber Incident and Dispute Data, Version 1.5.”

⁷¹ Adapted from Council on Foreign Relations, “Tracking State-Sponsored Cyberattacks Around the World”; Adapted from Maness, Valeriano, and Jensen, “The Dyadic Cyber Incident and Dispute Data, Version 1.5.”

⁷² Adapted from Council on Foreign Relations; Adapted from Maness, Valeriano, and Jensen.

pursue national objectives, corresponds with the increase in Level 3 incidents.⁷³ The ability to target and exfiltrate information from specific network, provides opportunity for intelligence collection, and it is not surprising that these types of incidents are increasing in frequency.

3. Conclusion

While this analysis of cyber incidents did not reveal a marked decline in the occurrence nor severity of State-backed cyber incidents targeting U.S. interests, some conclusions can be made. It appears that overall trends in the cyberspace domain likely outweigh any effects of a cybersecurity strategy. Trends that began as early as 2006 continue to impact security in the cyberspace domain. Specifically, an increase in the number of states pursuing objectives via the cyberspace domain, and ease of doing so, are the strongest drivers of the increase in volume of targeted attacks used to extract information.⁷⁴ However, the relative severity of the cyber incidents remained proportionally constant. This counters predictions of sharp increases in the severity of cyber incidents, and suggest that without the implementation of Defend Forward, cyber incidents could have been much worse over this period.

While Defend Forward may be more effective at providing security than a deterrent-based approach, the evidence points to the fact that the cyberspace domain is a rapidly evolving environment, and any security strategy must be agile and consistent to remain relevant. In contrast to a deterrence posture, Defend Forward may offer the flexibility and potential for the consistency needed to be impactful. This impact, however, cannot be observed from evidence during the first four years of its implementation.

⁷³ Council on Foreign Relations, “Tracking State-Sponsored Cyberattacks Around the World.”

⁷⁴ Alex Scroxton, “Nation-State Cyber Attacks Double in Three Years,” ComputerWeekly.com, April 8, 2021, <https://www.computerweekly.com/news/252499042/Nation-state-cyber-attacks-double-in-three-years>.

B. IMMEDIATE EFFECTS ON STABILITY

The definition of stability drafted by the GCSC in 2019 states that it is a condition in which “everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.”⁷⁵ This definition can be broken down into four criteria that must be met to achieve a stable domain.

1. Assured availability of cyberspace services and information
2. Assured integrity of cyberspace services and information
3. Change in the domain is managed in relative peace
4. Tensions are resolved in a non-escalatory manner

To assess the immediate effects of Defend Forward in relation to stability, this section identifies the presence or absence of tangible indicators of these four criteria in real world examples to assess any effect Defend Forward has had thus far on promoting or impeding a stable environment.

1. Tangible Indicators of Stability Criteria Being Met

Before assessing Defend Forward’s potential impact on the stability of the cyberspace domain, it was imperative to identify what trends or events would indicate movement toward or away from the four criteria being met. With these trends or events identified, the extent to which Defend Forward played in achieving them can then be assessed.

a. Assured Availability

The first criteria for stability is that there must be assured availability of cyberspace services and information. In other words, capabilities and information stored in the cyberspace domain must be readily available to users who need access and the owners of

⁷⁵ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 13.

the information. This would entail the elimination of ransomware and denial of service attacks as a viable tactic for malicious actors operating in the domain. In a ransomware attack, the malicious user encrypts or prevents the victim from accessing systems or information, this is followed by a demand for payment in return for returning access. Ransomware attacks by their nature are a malicious means to deny availability. Furthermore, they have proven to be a viable means of attacks for criminal and non-state actors to raise money, as in many cases ransoms are met.⁷⁶ Similarly denial of service attacks targets the availability of information and services in the cyberspace domain, by various means, but commonly by flooding the victim with large amounts of unsolicited packets of information. This overwhelms the system's ability to process the bogus information and prevents legitimate use of the system.

Another indicator that this criterion is being met, or that the cyberspace domain is getting closer to achieving this criterion, is the implementation of laws and policies whose aim is to protect the core of the internet. The core of the internet is defined by the GCSC as including “packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media.”⁷⁷ These physical and logical components and functions enable the functioning of the internet as an interconnected network of networks, and as such availability in the cyberspace domain is critically dependent on them. Laws and policies designed to protect the core of the internet are inherently difficult to implement, as there is no single owner of the core. The Aspen Institute outlined these difficulties in 2020 describing the three main obstacles to achieving security for the core of the internet.

- *No one in charge*: There is no single organization responsible for protecting the public core. Efforts to improve its security and stability depend on global coordination between a variety of stakeholders, some

⁷⁶ Lynsey Jeffrey, “Why Ransomware Attacks Are on the Rise — and What Can Be Done to Stop Them,” PBS NewsHour, July 8, 2021, <https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them>.

⁷⁷ Global Commission on the Stability of Cyberspace, *Definition of the Public Core of the Internet*, (Bratislava: The Hague Center, May 2018), <https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf>, 1.

with opposing interests. Furthermore, different groups control different parts of the public core, making coordination more difficult.

- *Privately-owned commons* – The public core is generally managed by private companies and international nonprofits. Government agencies play a marginal role in managing or overseeing the public core, leading many to dismiss the role of federal policy in securing the public core.
- *No first-mover advantage*: The Internet generates network effects that create a strong disincentive to be the first organization to adopt a new standard or protocol that might enhance security for some element of the public core. Yet adoption is only effective if many or all organizations participate as well.⁷⁸

Because of the multistakeholders nature of the problem, international agreements regarding protection of the internet core could be a key indicator of moving toward achieving guarantees of access in the cyberspace domain.

b. Assured integrity

The integrity of information and the services that information enables is critical to the functioning of the cyberspace domain. As such, having assured integrity of services and information in the cyberspace domain is a necessity to achieve stability in the domain. Integrity provides a guarantee that information stored or routed through the cyberspace domain remains unaltered outside of intentional alteration by the owner. Integrity can be compromised by unintended aspects of the domain, such as congestion of information traveling on a shared medium in certain situations, or maliciously by actors intending to corrupt or alter data to prevent it from being used as intended.

To measure changes in the level of assurance of integrity, the behavior of the user can be examined. It is difficult to quantify the amount to which assurance of integrity changes, however if integrity assurance sharply declines, this could be seen by a sharp decline of reliance on the cyberspace domain to store or communicate data. Conversely, if assurances of integrity are rising, it can be expected that use of the cyberspace domain to communicate and store data will increase. Therefore, if increases in the use of the

⁷⁸ “A National Cybersecurity Agenda for Resilient Digital Infrastructure,” The Aspen Institute, December 2, 2020, <https://www.aspeninstitute.org/longform/a-national-cybersecurity-agenda-for-resilient-digital-infrastructure/securing-the-internets-public-core/>.

cyberspace domain, specifically the internet and cloud infrastructure, to store and communicate information exist, it can be assessed that integrity in the cyberspace domain is not diminishing. This indicator is not perfect, however. If the user is willing to take on more risk, then an increase of usage may not indicate an increased guarantee of integrity but may indicate increased need or desire to use the cyberspace domain to store and communicate information, despite assurances of integrity. This increase in risk tolerance would become more and more of a factor as economic and social pressures to use the cyberspace domain increase. At a macro-level though, increased usage can be used as an indicator for general trust in the assurance of integrity in the domain.

c. Management of Change

A hallmark of a stable environment is that change is handled peacefully, and stakeholders agree on courses of action to manage change. As such, this is a criterion to achieve the stability defined by the GCSC. Evidence of the peaceful management of change in the cyberspace domain can be seen in multilateral agreements between stakeholders, to include international agreements between States. While the former is inclusive of the latter, the cyberspace domain is unique in that many of the stakeholders are private industries and not nation states. Thus, the adoption of standards to manage new technology and capabilities, is as much an indicator of the peaceful management of change, as international agreements between States which govern behavior and practices of those States.

d. Tension Resolution without Escalation

The lack of escalation from tension in the cyberspace domain goes hand in hand with the peaceful management of change. If disagreements escalate vertically into offensive actions in the cyberspace domain or horizontally into other domains, then stability cannot be achieved. For this reason, if there is evidence of escalatory activity in the cyberspace domain or directly resultant from tensions in the cyberspace domain, then this is an indicator that stability is not achieved. Furthermore, if these escalatory actions are conducted at an accelerated rate, then this could indicate the domain is moving farther from stability.

2. Does Defend Forward Impact the Criteria for Stability?

Once the real-world indicators of progress toward stability are identified, the task then becomes determining whether Defend Forward can be linked to those indicators to determine the impact that Defend Forward is having on achieving stability in the cyberspace domain. This study of the effects of Defend Forward illuminated the role of this strategy in regard to stability in the cyberspace domain from 2018 to the present in 2022. The nature of the results prompts greater questions as to what, if any, effects Defend Forward will have on the prospect of long-term stability of the domain.

a. Defend Forward and Assured Availability

As described above, assured availability in the cyberspace domain can be assessed by the presence or absence of successful attacks on the availability of information or services. Chief amongst these attacks are the ransomware attacks perpetrated by criminal and nonstate actors in the cyberspace domain. Ransomware attacks are a priority to defend against for the U.S. Government, as they pose a serious risk to the availability of services necessary for many critical U.S. interests.⁷⁹ In addition to Ransomware, denial of service attacks are an additional threat to U.S. interests in the cyberspace domain. Like ransomware attacks, they deny availability to users, and have proven a successful tactic for state and nonstate actors to attack U.S. interests.⁸⁰

As both types of attacks on availability have been used to target U.S. interests, providing defense against them is part of the security goals of Defend Forward. Therefore, if Defend Forward is successful in securing U.S. interests from these attacks, Defend Forward is also making progress to fulfil the criteria of assured availability for the United States.

⁷⁹ U.S. Department of Defense, “National Cyber Strategy,” 4.

⁸⁰ “Denial of Service Attacks against U.S. Banks in 2012–2013,” Council on Foreign Relations, Accessed April 10, 2022, <https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013>.

From 2018–2021, there were no major denial of service or ransomware attacks against U.S. interests attributed to State actors.⁸¹ This is contrasted against major Denial of Service attacks that occurred before Defend Forward, such as the 2013 denial of service attacks against U.S. financial institutions.⁸² This would suggest that Defend Forward is successfully defending against these types of attacks against U.S. interests. However, regarding non-state actors, ransomware attacks remain a viable attack vector. The 2021 ransomware attack against Colonial Pipeline, perpetrated by DarkSide a Russian criminal organization, forced the shutdown of a major U.S. oil pipeline in the southeast United States. Furthermore, Colonial Pipeline paid the ransom to DarkSide to restore the availability of their systems, proving ransomware attacks are a viable means to make profit in the cyberspace domain.⁸³ The U.S. failed to defend against or prevent this attack, and given the strategic impact it had on U.S. critical infrastructure, it becomes clear that the criterion for assured availability is not met.

Defend Forward may be making progress in assuring availability to U.S. interests, but as documented in the Council of Foreign relations database, there are still numerous examples of availability attacks occurring around the world.⁸⁴ For this reason there is no real evidence that Defend Forward is making substantial progress in securing availability worldwide. It is also worth noting that securing availability is not the stated mission of the strategy.⁸⁵ At this point in time it is unclear if Defend Forward is making a significant impact on global trends of availability attacks.

Another indicator of assured availability is agreements protecting the core of the internet. The pool of resources and process on which the internet as whole relies on. While international organizations such as the GSCS agree in theory on the need to protect the

⁸¹ Council on Foreign Relations, “Tracking State-Sponsored Cyberattacks Around the World.”

⁸² Council on Foreign Relations, “Denial of Service Attacks against U.S. U.S. Banks in 2012–2013.”

⁸³ William Turton, Michael Riley, and Jennifer Jacob, “Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom,” *Bloomberg*, May 13, 2021, <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>.

⁸⁴ Council on Foreign Relations, “Tracking State-Sponsored Cyberattacks Around the World.”

⁸⁵ U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, 7.

availability of the internet core, there is little evidence of meaningful agreements between states or private stakeholders to provide enforceable assurance of availability. Furthermore, there is even less evidence that Defend Forward is prompting or preventing such agreements. As such, it cannot be determined at this point if Defend Forward is making an impact on multistakeholder agreements assuring the availability of the internet core.

b. Defend Forward and Assured Integrity

The criterion of assured integrity is a measure of the trust users place in the cyberspace domain. If users can trust that their data is secure from alteration, they are more willing to use the cyberspace domain to store and communicate that data. Defend Forward's mission is to secure the cyberspace domain for U.S. interests, and that includes securing data and services from illicit alteration.⁸⁶ As such, if Defend Forward is improving assurances of integrity in the cyberspace domain for U.S. interests, use of the domain to store and communicate data will likely increase in the United States.

It is certain that users in the United States have continued to increase their use of the internet and the cyberspace domain at large to communicate. Similarly, the use of cloud-based infrastructures to store information and provide services continues to grow as well with U.S. users.⁸⁷ What is less certain is the effect that Defend Forward has had since 2018 on promoting this use. Without tangible statistics, it is impossible to ascertain the exact degree to which the strategy plays in increases of assurances of integrity. However, what can be said is that usage continues to increase as services become more expansive, and available. This suggests that in the U.S. the Defend Forward strategy is, if nothing less, not decreasing assurances in the integrity of data in the cyberspace domain.

⁸⁶ U.S. Cyber Command, 2.

⁸⁷ The Brainy Insights, "Cloud Storage Market to Reach USD 353.81 Billion and Exhibit at a CAGR of 24.48% from 2021 to 2028," GlobeNewswire, January 20, 2022, <https://www.globenewswire.com/news-release/2022/01/20/2369910/0/en/Cloud-Storage-Market-to-Reach-USD-353-81-billion-and-Exhibit-at-a-CAGR-of-24-48-from-2021-to-2028-The-Brainy-Insights.html>.

At this time, it is unclear if Defend Forward has influenced global perceptions of integrity in the cyberspace domain since its implementation. What can be ascertained is that there has not been a radical shift in improved integrity in the cyberspace domain since 2018. While it cannot be assessed that Defend Forward has improved or decreased perceptions of, or actual assurances of integrity, it can be assessed that it has not affected either in a radical fashion.

While assured integrity is a hallmark of stability per the GCSC, stability is not the goal of Defend Forward. This makes such comparisons difficult to make, as the nebulous relationship Defend Forward has with integrity in the cyberspace domain at a global scale makes understanding that relationship impractical in the short term. While assured integrity is a criterion for stability, it is problematic to assess that increases in perceptions of assured integrity can be attributed to Defend Forward. However, there is no evidence suggesting that Defend Forward is decreasing perceptions of integrity, and thus decreasing this indicator of stabilization.

c. Defend Forward and Change Management

To achieve stability in the cyberspace domain, change must be managed peacefully. This management must be done by all stakeholders to include private industry as well as traditional nation states and can be seen in international agreements and in industry standards of practice. To measure the extent to which Defend Forward has affected this process in the short term, a link must be found between the two.

In the cyberspace domain, international standards that govern the functioning of the domain are critical for the development and stability of the interconnected domain. As technology and capabilities evolve, these standards and the organizations that govern them must keep pace to adapt and evolve the protocols and infrastructure demanded by the advancing domain. Organizations such as the Internet Corporation of Assigned Names and Numbers (ICANN) attempt to standardize the protocols and technology required for the

cyberspace domain to function, and as such manage change within the domain. This is a key aspect and criterion for achieving stability in cyberspace.⁸⁸

However, there is disagreement amongst nations regarding the implementation of standards to manage change. Specifically, China is taking an active role in defining its own standards as part of a campaign to become a “Cyber Great Power.”⁸⁹ This creates alternate standards and prevents domain-wide standardization, which in turn prevents a uniform mechanism to adapt to change. This is a move away from the system of protocol management that has existed since the early day of the internet. Industry and nations have benefited from adhering to universal standards, but with geopolitical state actors becoming more directly involved in developing standards and protocols, and the processes that govern them, domain stabilization becomes more difficult.⁹⁰

This balkanization of internet standards is not dependent on specific cyber defense strategies but is likely symptomatic of larger great power competition. As such, Defend Forward is not a sole cause for this trend, which precedes that policy. At its essence, Defend Forward, and thus the security of U.S. interests, benefits from promoting standardization of protocols and the orderly and holistic management of change in the cyberspace domain. Universal change management allows USCYBERCOM better access to create friction for adversaries and makes the domain more predictable. The management of change in the cyberspace domain may be becoming more difficult with a breakdown of universal protocols and processes, but this is not a direct result of Defend Forward. Defend Forward does not prevent universal standards to manage change in the cyberspace domain. Rather, interstate competition, to which Defend Forward is also a response, is pushing the domain away from this measure of stabilization.

⁸⁸ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 13.

⁸⁹ Joshua Park, “Breaking the Internet: China-U.S. Competition Over Technology Standards,” *The Diplomat*, February 9, 2022, <https://thediplomat.com/2022/02/breaking-the-internet-china-us-competition-over-technology-standards/>.

⁹⁰ “Open Internet Standards,” Internet Society, Accessed April 10, 2022, <https://www.internetsociety.org/issues/open-internet-standards/>.

Large scale international agreements, especially multi-lateral agreements regarding the cyber space domain, are a key indicator peaceful management of change is occurring. Such agreements provide an infrastructure by which change can be managed in an organized way. In November 2021, the U.S. joined an 80-country “Paris Call for Trust and Security in Cyberspace.” This agreement “welcome [s] collaboration among governments, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections.”⁹¹ Multilateral Agreements like this provide a backbone from which change can be managed. As the U.S. signed this agreement with 80 other countries, it can be argued that there was a tacit acceptance of U.S. security and defense strategies in the cyberspace domain. For this reason, it can also be argued that Defend Forward has not had a negative role in the formation of international agreements.

As promising as agreements like the Paris Call sound, they do not incorporate the entirety of stakeholders in the cyberspace domain. Actors like China and Russia may not subscribe to the liberal models of international cyber order, and thus their effectiveness of moving the domain toward stability may be suspect.

Since its implementation, Defend Forward has not prevented the development of international agreements, or industries’ standards of practice to manage change. Yet, the goal of universal and holistic management of change in the cyberspace domain may be even farther away than in years past, as states like China take a more direct role in directing the creation of standards to increase their own influence over the domain. The development of international agreements and standards is a long-term process, and at this time there is not enough evidence to declare that Defend Forward influences these developments. Managing change in the cyberspace domain is influenced by many geopolitical stakeholders, and the defense strategy of one state may not have a major impact on this development.

⁹¹ “The Paris Call for Trust and Security in Cyberspace,” Paris Call, November 12, 2018, <https://pariscall.international/en/call>.

d. Defend Forward and Non-Escalation

The final criterion for stability in the cyberspace domain, per the GCSC definition, is that tensions cannot escalate. This escalation can be vertical, prompting retaliatory cyberattacks of increased severity; or horizontal, prompting retaliatory actions outside of the cyberspace domain. The issue of escalation is a key concern of many critics of Defend Forward, arguing that by creating friction the U.S. invites escalatory responses.⁹²

This concern, however, does not seem to be the case thus far. If Defend Forward were to cause escalation, there should be evidence of attacks against U.S. interests, directly tied to U.S. persistent engagement in the domain. In terms of vertical escalation, the Council of Foreign Relations dataset does not show any incident targeting a U.S. interest that can be tied directly back to USCYBERCOM friction causing operation.⁹³ Horizontal escalation attributed to USCYBERCOM persistent engagement would equally be evidence that Defend Forward worked against stability in the cyberspace domain. However, there is no evidence that any action taken against a U.S. interest outside the cyberspace domain can be identified specifically as a reaction to Defend Forward. This is not to say that escalation cannot occur gradually over time and may not be identifiable in the four years Defend Forward has been in place. For this reason, an assessment finding no link of Defend Forward to escalation cannot be made by looking only at the immediate effects of the strategy. In the short term, however, there is no evidence of escalatory response to Defend Forward.

3. Conclusion

From analyzing Defend Forward's immediate effects on the criteria for stability, it can be assessed that Defend Forward has little impact on the stability of cyberspace in the short-term. As detailed above, there is little evidence that it prevents stabilization, but there is also little evidence that the strategy actively moves the domain closer to stability. Based on the definition of stability from the GCSC, four criteria were identified that would be

⁹² Fischerkeller and Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace."

⁹³ Council on Foreign Relations, "Tracking State-Sponsored Cyberattacks Around the World."

necessary for stability. Assessing real-world indicators of assured availability, assured integrity, change management, and non-escalatory tension resolution, supports the conclusion that Defend Forward does not seem to be affecting these measures significantly in the short-term. Analysis of the potential long-term effects of Defend Forward will shed greater light on the potential relationship between Defend Forward and stability. Specifically, analysis of long-term effects will provide greater insight to the effectiveness of Defend Forward at providing security for U.S. interests if it is not actively supporting the development of stability.

C. CONCLUSION

While in the short-term Defend Forward has shown itself to likely be effective at increasing security for U.S. interests, overall trends of increased offensive cyber activity in the domain continue. Incidents targeting the U.S. continue to increase, though the severity does not. As security is the goal of Defend Forward, it appears the strategy is more effective than the previous security strategy. Simultaneously, Defend Forward generally has had little effect on the stability of the cyberspace domain one way or the other. This is not to say that it is detrimental to the stability of the domain, only that it does not appear to move the domain toward nor away from stability. Taken together, analysis of the short-term effects of Defend Forward show that it is not a major influence on domain-wide trends thus far. The number of cyber-attacks against U.S. interests continues to grow, albeit potentially at reduced rate, and the cyberspace domain as a whole does not seem to be pushed toward or away from stability by Defend Forward.

This conclusion suggests that the impact the Defend Forward has on the cyberspace domain is not as significant as some theoreticians and critics portray. In the short-term however, Defend Forward does show promise at improving the security of U.S. interests. As neither security nor stability are modest goals, analysis of the long-term effects of Defend Forward on security and stability may shed light on whether the short-term effects will continue over the long run, and thus the overall impact of the strategy on security and stability.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LONG-TERM EFFECTS ON CYBERSECURITY AND CYBERSPACE DOMAIN STABILITY

While the short-term effects of Defend Forward were shown to likely provide better security than the previous deterrence strategy, Defend Forward also appeared to have little immediate effect on the stability of the cyberspace domain. To fully analyze the effects of Defend Forward, an assessment of projected long-term effects to both security of U.S. interest and stability of the cyberspace domain is necessary.

To assess these long-term effects on security, this study analyzes the unique difficulties faced when implementing a defensive strategy in an ill-defined and ever-evolving domain. The need for a flexible and yet consistent approach to disincentivizing adversarial belligerence is critical in this environment to achieving security. With this in mind, Section A evaluates Defend Forward to determine the likelihood of long-term success in providing security to U.S. interests.

To assess the likely effects of Defend Forward on the long-term stability of the cyberspace domain, this study utilizes the eight specific behavioral norms outlined by the GCSC as required to reach stability in the domain. To achieve stability, according to the GCSC, these norms must be voluntarily adopted and implemented by the multistakeholders of the domain. Section B describes each of these eight norms and evaluates how Defend Forward, as an instrument of U.S. security policy, could influence other stakeholders' behavior relative to adoption of these norms. By assessing the effects of Defend Forward on the formation of each of these norms, this study can project the likely effects that Defend Forward will have on the long-term stability of the domain.

A. SECURITY IN THE LONG-TERM

One of the most significant effective changes in moving from a deterrence paradigm of cyber defense is the ability for the U.S. to act consistently in a persistent engagement paradigm. As pointed out, one of the key failures of the deterrence strategy in the cyberspace domain was the inconsistency of response action by the U.S. This generated uncertainty for adversaries as to whether they would face response actions for carrying out

an operation against U.S. interests. Response hesitancy was largely due to the risk that cyber response actions could escalate an incident into armed conflict.⁹⁴ This perception existed because the deterrence strategy was designed to counter operations in cyberspace that fell within the realm of armed conflict, and thus responding cyber actions would be proportional. In other words, the cyberspace domain was treated merely as an extension of the physical battlefield. Responding to an attack that fell below the level of armed conflict with a corresponding response action seemingly risked escalation of hostilities and was thus unappetizing. However, as illustrated by the 2013 Iranian attacks against U.S. financial institutions, and Russian use of the cyberspace domain to interfere with the 2016 U.S. Presidential elections, cyber actions taken against U.S. interests that are below the threshold of armed conflict can and do have strategic effects against U.S. interests.⁹⁵ In these two cases, the attacks were not deterred and this can be attributed to the attackers not believing they would face a response action or be held accountable by the U.S. The lack of consistency and unwillingness to risk escalation crippled deterrence as a defense strategy in cyberspace.

Persistent engagement and Defend Forward are designed to offer much more flexibility to the U.S. One of the intended effects of Defend Forward is to increase flexibility of action by enabling USCYBERCOM to be proactive, present in the environment, and engaging with adversaries. This allows USCYBERCOM to act below the threshold of armed conflict, to de-incentivize attacks that also fall below this threshold, thus causing friction for adversaries with reduced risk of escalating interactions to the level of armed conflict. Persistent engagement offers an option for policy makers to use cyber operations in a non-escalatory manner. Persistent engagement also enabled Congress to “clarify the statutory authority for military cyber operations to enable Cyber Command to conduct traditional military activities in addition to the mostly preparatory operations to

⁹⁴ Nakasone, “Introduction: A Cyber Force for Persistent Operations,” 3.

⁹⁵ Nakasone, 3.

which it had been limited previously,” and the drafting of the 2018 National Cyber Strategy.⁹⁶

The flexibility to act enables cyber commanders to actively engage with adversaries with means and motivation to attack U.S. interests in the cyberspace domain more consistently. With this comes the assumption that U.S. operators can effectively identify the malicious actors, their cyber persona, and where within the physical and logical cyberspace domain they are operating.

Flexibility and the ability to be consistent are critical to maximize security in the cyberspace domain. The flexibility and consistency which Defend Forward affords allows for greater long-term security for U.S. interests in the cyberspace domain. The rapid pace at which technology evolves, coupled with low cost of entry and widespread dispersal of interests and adversaries, presents a rapidly moving target to achieve security. Deterrence failed at hitting this target but Defend Forward affords the flexibility and consistency required for security success in the long-run. However, if in pursuit of security, Defend Forward prevents stabilization by flaunting norms of behavior favored by the international community, it raises the question of whether long-term security gains will ultimately be sacrificed by creating a more unpredictable and ultimately less secure domain.

B. STABILITY IN THE LONG-TERM

As shown, much of the debate surrounding the efficacy of Defend Forward centers around the perceived danger of destabilization of the cyberspace domain. As proposed by the GCSC, stability in cyberspace is achieved by the multistakeholder adoption and voluntary acceptance of defined norms of behavior. That stability is a vision of a domain in which “everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.”⁹⁷ If stability was the long-

⁹⁶ Fischerkeller and Harknett, “Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace.”

⁹⁷ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 13.

term goal of Defend Forward, the strategy should not hamper the adoption of these norms, and even work to strengthen and embolden them.

Security, however, not stability, is the goal of Defend Forward. But if in pursuing security, the strategy breaks the norms of behavior through its proactive tactics, then critics argue ultimately the strategy is self-defeating, as this will preclude stabilization of the domain that long-term U.S. security requires. This critique is due to the implicit association of stability to long-term security that the analysis of this thesis is distinguishing. By making this distinction explicit, it becomes possible to evaluate whether and to what degree promotion of long-term cyberspace stability serves long-term U.S. security interests, and what influence persistent engagement from USCYBERCOM may have to either promote or detract from the growth of norms such as those proposed by the GCSC.

1. Stabilization Through Cooperative Norms

The GCSC envisions the stabilization of the cyberspace domain through the adoption of cooperative norms of behavior, which the multiple stakeholders of the domain will be willing adopt. Through adoption of these norms, behavior in the domain becomes more predictable, and the domain ultimately reaches an equilibrium into the GCSC's envisioned stability. The stakeholders will be willing to adopt these norms because stability, the GCSC argues, will be mutually beneficial to all parties.

The GCSC proposed norms of behavior are as follows:

1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.
2. State and non-state actors must not pursue, support, or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.
3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.
4. State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

5. States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.
6. Developers and producers of products and services on which the stability of cyberspace depends should prioritize security.
7. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.
8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.⁹⁸

Using these norms as a benchmark, Defend Forward can be analyzed to understand its relationship to the norms, and ultimately its relationship to the creation of stability in the cyberspace domain. If the eight cooperative norms promulgated by the GCSC are the prerequisites and means to achieve stability, then a strategy that actively prevents the adoption of these norms, is counterproductive to the evolution of a stable domain. Healey argues that Defend Forward has the potential to be this counterproductive element and work to destabilize the domain if adequate safeguards and feedback mechanisms are not in place and utilized.⁹⁹ However, the following assessment of Defend Forward's relationship to these norms suggests that Defend Forward would not prevent stabilization in the long-term but would also have little effect on the stabilization of the domain as a whole.

Healey is correct that a judicious if not cautious application of Defend Forward is necessary if the strategy is to support stability.¹⁰⁰ An overzealous application of creating friction is sure to alienate stakeholders in the cyberspace domain, sure as an underwhelming application will be ineffective at creating security. However, a judicious application of Defend Forward would not violate the majority of the eight norms set forth. In fact, norm development would specifically be aided by the U.S. providing enhanced security to U.S. interests via Defend Forward.

⁹⁸ Global Commission on the Stability of Cyberspace, 21.

⁹⁹ Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," 10.

¹⁰⁰ Healey, 12.

2. Defend Forward and Stabilizing Norms

As discussed in Chapter 2, maintaining the availability and integrity of the internet core is advantageous to U.S. interests, convergent with the first GCSC proposed norm to create stability. The core of the internet is a shared resource on which not only U.S. interests rely, but the functioning of the cyberspace domain relies on the availability of the core to provide global communication and connectivity.¹⁰¹ By proactively causing friction for those who would deny availability of or integrity in the internet core, malicious actors are disincentivized from violating the security of the internet core. Through this action, Defend Forward increases the security of U.S. interests, but also supports the development of the norm of protecting the shared resource of the internet core.

USCYBERCOM is mandated to defend free and legitimate U.S. elections.¹⁰² This mandate advances the second GCSC norm, at least defensively. Elections and the confidence in democratic institutions is an enticing target. As Russian activity in the 2016 U.S. Presidential election showed, the cyberspace domain is a powerful vector to delegitimize and/or degrade the political cohesion of the United States.¹⁰³ As purported by the DOD, Defend Forward is well postured to increase the security of elections, through persistent engagement with malicious actors, and thus provides a model of security that supports this norm.¹⁰⁴

The third GCSC norm can also be supported by maximizing supply chain security for components and systems used in the cyberspace domain. The supply chains for critical

¹⁰¹ Global Commission on the Stability of Cyberspace, *Call to Protect the Public Core of the Internet* (New Delhi: The Hague Centre for Strategic Studies, EastWest Institute, 2017), <https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf>, 1

¹⁰² U.S. Cyber Command, “Our Mission and Vision.”

¹⁰³ United States Senate. *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 Presidential Election. Volume 2: Russia’s Use of Social Media with Additional Views*, report 116-XX (Washington, DC: 116th Congress 1st Session), Accessed February 18, 2022. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

¹⁰⁴ David Vergun, “Cybercom’s Partnership with NSA Helped Secure U.S. Elections.” *U.S. Department of Defense News*, March 25, 2021, <https://www.defense.gov/News/News-Stories/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/>.

U.S. components are critical to U.S. economic and defense interests which rely on trustworthy systems to interact in the cyberspace domain. By creating friction for those intending to attack these systems in production, such attacks are disincentivized. This aligns with and supports the GCSC norm: preventing the tampering of “products and services in development and production” which could “substantially impair the stability of cyberspace.”¹⁰⁵

The fourth GCSC norm would prevent the use of botnets comprised of the general public’s resources.¹⁰⁶ Botnet attacks are used against U.S. interests in the cyberspace domain, such as the 2013 Iranian attacks on the U.S. financial sector.¹⁰⁷ As such, Defend Forward should defend against such attacks to maximize the security of U.S. interests. Creating friction for conducting botnet attacks supports U.S. security, and reducing the ease of such attacks contributes to the formation of this norm.

The disclosure of vulnerabilities is a key tactic available to USCYBERCOM to create friction as a part of Defend Forward. If a threat is detected, USCYBERCOM can work with private industry partners to identify and/or patch vulnerabilities that may be targeted. By disclosing the vulnerability to be patched, USCYBERCOM makes the job of the would-be attacker more difficult, as that vector of attack is no longer viable. This tactic would support not only security of U.S. interests but would support the fifth norm as well. As stated in the norm, these disclosures should be the default behavior, which would serve both a persistent engagement defense strategy and as a stabilizing move.

The GCSC’s sixth norm puts priority on security in the development of products and services. While a persistent engagement strategy does not directly support this, it goes hand in hand with a defense strategy. Security best practices incorporated in the development of systems makes a defense strategy more effective, as systems are more difficult to attack, and thus there is less incentive to attack. This is articulated by USCYBERCOM in its 2018 Command Vision, by highlighting the importance of the

¹⁰⁵ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 21.

¹⁰⁶ Global Commission on the Stability of Cyberspace, 21.

¹⁰⁷ Council on Foreign Relations, “Denial of Service Attacks against U.S. Banks in 2012–2013.”

resiliency of DOD systems, which must be designed to be secure.¹⁰⁸ Defend Forward relies on the prioritization of security in systems, as part of a holistic approach to security and defense. As such, Defend Forward and the GCSC norm are mutually supportive.

The penultimate GCSC norm proposes a standard of cyber hygiene: “a regime of foundational measures that represent prioritized, essential tasks to perform to defend against, prevent and rapidly mitigate avoidable dangers in cyberspace.”¹⁰⁹ USCYBERCOM operates under similar ideas articulated in its Command Focus: “USCYBERCOM improves DOD’s capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM is designing the cyber force structure, training requirements and certification standards that will enable the Services to build the cyber force required to execute our assigned missions.”¹¹⁰ The use of best practices to operate in the cyberspace domain effectively and securely is supported by USCYBERCOM as an enabler to a successful persistent engagement strategy. Thus, this norm is supported by the Defend Forward strategy.

The final GCSC norm prohibits offensive cyber operations by nonstate actors and prescribes state actors to prevent such offensive cyber operations. This norm is directly supported by Defend Forward. Attacks by non-state actors are a proven threat to the security of U.S. interests. Cyber-attacks from criminal organizations such as the 2021 Colonial Pipeline ransomware attack illustrate the threat that non-state actors pose toward U.S. security in cyberspace. As Defend Forward strives to create friction and disincentivize offensive action against U.S. interests in cyberspace, the strategy will by necessity have to target non-state actors in the domain. This is exactly what is described in the norm.

In the long-term, Defend Forward can assist in the development of norms, as well as maximizing security of U.S. interests. The key is in finding a balance. Creating friction

¹⁰⁸ U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, 7.

¹⁰⁹ “GCSC Proposed Norms of Responsible Behavior in Cyberspace.” Global Commission for the Stability of Cyberspace, accessed April 30, 2022, <https://cyberstability.org/norms/>.

¹¹⁰ U.S. Cyber Command “Our Mission and Vision.”

must disincentivize malicious behavior against U.S. interests, but at the same time protect the common shared resources, and model responsible behavior in the domain. This dual purpose does not decrease the effectiveness of the strategy in providing security, as protection of shared resources and modeling desired behavior serves both objectives.

The preceding evaluation of long-term persistent engagement and norm development suggests that, in and of itself, Defend Forward should not tend to prevent stabilization of the cyberspace domain, and in fact will generally support the development of all the required norms. However as stated, the objective of Defend Forward is security, and this objective is well placed. While Defend Forward may support stabilization of the domain in the long run, stabilization as a goal would likely be ineffective. The structural characteristics of cyberspace make its inherent instability a defining aspect of the domain (as discussed further below). Hence, promoting stability is not a prerequisite to U.S. pursuit of its cyber security interests, but it can be a supportive adjunct to that pursuit, and improved stability may be a beneficial consequence as well.

3. Defend Forward, Stability, and Unique Cyber Features

In traditional domains, stability prevents uncertainty, and uncertainty is a security risk, as there are no norms of behavior. However, this does not seem to apply directly to the cyberspace domain. The cyberspace domain is defined by several characteristics that make stability unrealistic. Rapid evolution and development, anonymity, and a low cost of entry are the structural components that in-part form the unique nature of the cyberspace domain. These structural characteristics of the domain, make the development of norms of behavior incredibly difficult, and ultimately make reaching stability a near impossibility in the long-term.

Unlike in physical domains, rapid evolution of technology, and the behaviors that it enables, consistently and rapidly change the landscape of the cyberspace domain. In physical domains, such as the maritime domain, technology and capabilities have evolved over generations, but generally the functions and landscape of the maritime domain remain constant. It is a means to transport goods and people and is a source of physical resources. In contrast, the cyberspace domain in just the past twenty years has changed remarkably.

The computing and communication advances that enable today's use of the cyberspace domain, are a far cry from the early days of the Internet.¹¹¹ This rapid evolution of technology and behavior makes technology enabled behavior difficult to predict, and always in a state of flux. This in turn makes stabilization through norms difficult, as the conditions of tomorrow may not align to the behavior of today. A realist approach would suggest that as technology evolves, malicious actors will seek to use newly enabled capabilities to break existing norms for their own advantage and power. These constantly moving goal posts make maintaining norms of behavior very difficult and long-term stability unlikely.

Anonymity also makes establishing norms difficult in the cyberspace domain. Stability through norms requires there to be a means to deter violations of norms. This is problematic in the cyberspace domain because, as many have noted, attribution can be objectively difficult.¹¹² Not only can one person have a large number of cyber personas, but the ability to mask one's Internet Protocol (IP) address through any variety of means is relatively simple today. An IP address is a logical mechanism of IP, which is not tied to an individual, but assigned logically — not physically — to a device. Changing an IP address is a simple matter, and future capabilities may make this process even easier. It is very easy to identify who a warship belongs to in the maritime domain, it is far from trivial to identify a hacker in the real world behind a cyber-attack.

In the final norm, the GCSC details that to attain stability, non-state actors should not engage in offensive action in cyberspace, and State actors should respond to any such action.¹¹³ This logically makes sense. Offensive actions by non-state entities are inherently destabilizing to an established order. This is certainly true in the physical domain. Terrorist groups are an incredibly destabilizing factor, because they lack the stabilizing trappings that come with statehood and sovereignty, their behavior isn't tempered by the norms of

¹¹¹ Imre Dobák, "Thoughts on the Evolution of National Security in Cyberspace," *Security and Defence Quarterly* 33, no. 1 (March 1, 2021): 75–85. <https://doi.org/10.35467/sdq/133154>, 76.

¹¹² Clara Assumpcao, "The Problem of Cyber Attribution Between States," *E-International Relations*, May 6, 2020, <https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/>.

¹¹³ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 21.

the international community.¹¹⁴ The GCSC carries this notion into the cyberspace domain, where the problem is compounded by a much lower barrier to entry.

Compared to attacks in traditional domains, offensive cyber actions often require significantly less risk. Attacks like the 2021 Colonial Pipeline ransomware attack show that with little risk, a cyber-criminal organization can have strategic effects, and make a significant profit in ransom.¹¹⁵ As already demonstrated, deterrence does not prevent these types of attacks. When actors of unknown origin, with a minimal cost to entry are able to generate strategic effects via the cyberspace domain, it becomes extremely difficult to prevent such behavior. The risk-reward ratio favors the attacker and not the defender in these scenarios. This low barrier to entry will likely prevent the GCSC's final norm from ever being fully realized.

4. Conclusion

In the long run, Defend Forward will likely support the stabilizing of the cyberspace domain. All the required norms outlined by the GCSC are supported with the Defend Forward strategy. This is beneficial for the United States, as supporting stabilization builds international legitimacy for U.S. actions, which in turn can lead to agreements and cooperation. However, stability is unlikely to be achieved in the cyberspace domain in the long-run, and thus should not be the primary goal of Defend Forward. As a domain, cyberspace is unlike traditional domains. Its unique structural characteristics make the adoption and acceptance of norms by all stakeholders unlikely and unverifiable. Defend Forward however does support these norms, and as shown, the establishment and acceptance of several of these norms would directly benefit the security of U.S. interests. Long-term stability in a domain in constant flux, where attribution is difficult, and there are little to no barriers to entry, remains an elusive goal.

¹¹⁴ U.S. National Security Council, *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 17, 2002), <https://georgewbush-whitehouse.archives.gov/nsc/nssall.html>.

¹¹⁵ William Turton, Michael Riley, and Jennifer Jacobs. "Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom," *Bloomberg*, May 13, 2021, <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>.

C. CONCLUSION

In the long-term, Defend Forward will likely be an effective strategy. It offers the flexibility and consistency to enhance security of U.S. interests in a constantly evolving domain, while also supporting international norms that provide enhanced legitimacy for U.S. persistent engagement. From a security perspective, Defend Forward is uniquely suited to be successful in the cyberspace domain. The domain is in a state of constant evolution, and as such to have a successful security strategy, one must employ a level of agility to match the ever-evolving threats. Deterrence failed to this, because it was designed to defend against attacks above the threshold of armed conflict when the actual threats fell below this mark. This led U.S. administrations to inaction for fear of escalation, and ultimately an inconsistent and ineffective strategy. Defend Forward, however, allows proactive action below the threshold of armed conflict. Consistency of application created by proactive and persistent engagement with adversaries, coupled with the flexibility required to create friction dynamically, allows Defend Forward to be successful in the long run.

Defend Forward is often criticized as being destabilizing in a domain in which the stakeholders are trying to create stability. By assessing each of the norms proposed by the GCSC as required for long-term stability in the domain in relation to Defend Forward, this chapter has shown that Defend Forward in fact can support all the norms when applied judiciously. This is beneficial for the United States, not necessarily because Defend Forward is pushing the domain toward stability, but because these norms provide international legitimacy to U.S. persistent engagement. Increased international legitimacy can provide the United States the freedom to act more consistently in the cyberspace domain and potentially in concert with more allies, ultimately providing greater security.

Despite the benefits of supporting the GCSC norms, stability should not be the primary goal of Defend Forward. Security is the core objective and should be the core objective. Supporting the norms can provide legitimacy which has advantages, but they should not be supported in lieu of providing security for U.S. interests. Proponents of stability theory argue that by reaching a stable environment, security will be enhanced for all stakeholders. However, the structural characteristics of the cyberspace domain preclude

a stable environment. Rapid evolution of technology, a culture of anonymity, and a low barrier of entry ultimately make stability impossible in the cyberspace domain. As such, Defend Forward does not likely have, nor likely could have, a long-term effect on improving the stability of cyberspace. Attempting to mold the defense strategy to primarily reach this impossible goal would be faulty, and U.S. interests are better served by a persistent engagement strategy focusing on maximizing the security of U.S. interests.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. OVERALL EFFECTS OF DEFEND FORWARD

Defend Forward marks a paradigm shift for cyber defense strategy. The cyberspace domain is unique and distinct from traditional domains of warfare, and as such a new approach to defense was needed. Attempts to apply traditional deterrence strategy in the cyberspace domain failed because the means and ways of defense did not match the unique characteristics of the cyberspace domain. An attack in the cyberspace domain that remains below the level of armed conflict can have widespread strategic effects. However, response – or even threat of response – with attacks at the level of armed conflict risk escalation of conflict. This difficult position has inhibited the U.S. cyber deterrence strategy as decision makers were unwilling to risk escalatory response actions. Defend Forward provides a much stronger defense by persistently engaging with adversaries in the cyber space domain, causing friction below the level of armed conflict, and ultimately disincentivizing attacks on U.S. interests in the cyberspace domain.

Critics of Defend Forward argue that security gains from Defend Forward could be countered and outweighed by destabilizing effects in the cyberspace domain. They argue that persistent engagement could prevent norms of behavior from being established.¹¹⁶ Some also argue that this destabilization is particularly counterproductive because the creation of a stable environment in cyberspace will allow for the greatest level of security for U.S. interests.¹¹⁷ It is against this backdrop that this thesis set out to examine the effects of Defend Forward on both U.S. security and overall cyberspace stability.

To better ascertain the true effects of the Defend Forward strategy, this thesis began by breaking open the premise that U.S. security will automatically be higher in a stable environment. From this perspective, this thesis examined separately the strategy's effects on security of U.S. interests and effects on the stability of the cyberspace domain. By analyzing these effects since Defend Forward was implemented in 2018 through 2021, this

¹¹⁶ Fischerkeller and Harknett. "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace."

¹¹⁷ Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," 11.

thesis evaluated the immediate effects the strategy had on security and stability. By examining the unique characteristics of Defend Forward and applying them to the norms proposed by the GCSC for the cyberspace domain, this thesis was able to analyze the likely long-term effects of Defend Forward on both security and stability.

This thesis assessed that Defend Forward is likely, and will likely continue to be, an effective defense strategy in increasing the security of U.S. interests in the cyberspace domain. This thesis additionally concluded that Defend Forward generally supports both the principles of stability and the norms of behavior required for long term stability in the cyberspace domain as proposed by the GCSC. While this may seem to simply counter critics' objections over the destabilization of the cyberspace domain, this study revealed that the notion of stability in cyberspace is likely an unattainable goal. While supporting the principles and norms on which stability requires may give the U.S. international legitimacy in its actions, pursuing stability as a primary goal is faulty, as the structural characteristics of the cyberspace domain preclude enduring stability.

A. DEFEND FORWARD AND THE SECURITY OF U.S. INTERESTS IN THE CYBERSPACE DOMAIN

In both analyses of immediate and long-term effect on security, Defend Forward was shown to likely be effective at providing improved security for U.S. interests in the cyberspace domain. To ascertain the immediate effects on security, this thesis analyzed the Cyber Operations Tracker from the Council on Public Relations. This database includes all cyber incidents targeting U.S. interests from State or State affiliated actors from 2006 through 2021.¹¹⁸ By analyzing the quantity of incidents targeting the U.S. in 4-year groupings, the data clearly illustrated a growth in the number of cyber incidents targeting the U.S. from 2006 through 2021. This included an increase in the number of incidents from 2014–2017 to 2018–2021, with the implementation of Defend Forward as the dividing line between the two groupings. Straightaway this appears to show that Defend Forward was not effective at reducing the number of incidents targeting the U.S., let alone

¹¹⁸ Council on Foreign Relations. "Tracking State-Sponsored Cyberattacks Around the World."

not effective at increasing the security of U.S. interests. However, when viewed in a larger context, the increase in incidents between the two 4-year groupings is consistent with increases between every chronological 4-year grouping in the database. This suggests that Defend Forward at the very least was as effective as previous strategies. The data also show that the cyberspace domain is growing in attractiveness as a vector to attack U.S. interests.

To gain further insight, each incident in the Council on Foreign Relations database was assessed to determine the severity of the incident using the severity scale developed by Professor Ryan Maness at the Naval Postgraduate School.¹¹⁹ This assessment revealed that while the number of incidents increased between every chronological 4-year group, the severity of attacks held relatively constant. Specifically, most attacks in every grouping could be described at a level 3, with 1 being the least severe, and 10 being the most. This consistency contradicts multiple predictions based on global trends of increases in the severity of cyber-attacks against the U.S. made in 2018.¹²⁰ While this is far from conclusive, it does suggest that Defend Forward was likely successful in preventing more serious attacks against U.S. interests.

As Defend Forward has only been in effect since 2018, it was imperative to project out to assess the likely long-term effectiveness of the strategy in relation to its goal of securing U.S. interests in the cyberspace domain. To do this, the required characteristics of a successful defensive strategy in the cyberspace domain were assessed to be flexibility and consistency of action. Flexibility is important to be able to engage proportionally with adversaries in the domain, and consistency is vital to ensure uniform application of friction to adversaries. Deterrence-based models failed in the cyberspace domain because they were not capable to engage proportionally, and as a result there was inconsistent application of pressure. This inconsistency reduced the risk in the risk-reward balance of adversaries, ultimately putting U.S. interests at greater jeopardy.

¹¹⁹ Maness, Valeriano, and Jensen, “The Dyadic Cyber Incident and Dispute Data, Version 1.5.”

¹²⁰ Rosenzweig, “Cybersecurity Predictions for 2018”; DeNisco Rayome, “Forrester’s Top 6 Cybersecurity Predictions for 2018.”

Defend Forward is especially suited to provide security in the cyberspace domain, as persistent engagement is inherently consistent, and meets the adversary in red and grey network space to create friction below the level of armed conflict. This is the level at which most cyber-attacks occur, and proportionality of engagement is crucial to prevent escalation and enable consistency.

Overall, Defend Forward is likely to be effective at improving the security of U.S. interests in the cyberspace domain. This study was not conclusive, however. The cyberspace domain has many influencing factors that change at a rapid pace. This is evident by the continual annual increase in cyber incidents targeting U.S. interests in the domain. This study does show fairly conclusively though that Defend Forward is at least as successful as the previous deterrence strategy and is particularly well suited to be successful in the long run. By separating stability and security, the thesis was able to present a much clearer picture of the security effects of the strategy now and over time.

B. DEFEND FORWARD AND THE STABILITY OF THE CYBERSPACE DOMAIN

Through analysis of the immediate and long-term effects of Defend Forward, this thesis has concluded that Defend Forward has little effect on the stability of the cyberspace domain. The analysis reached this conclusion using the model of stability drafted by the GCSC, and the eight norms required to reach that state of stability, to assess any significant effects of Defend Forward on the development of stability by these measures.

To evaluate stability impact in the short-term, the GCSC definition of stability was broken down into four required criteria.

1. Assured availability of cyberspace services and information
2. Assured integrity of cyberspace services and information
3. Change in the domain is managed in relative peace
4. Tensions are resolved in a non-escalatory manner¹²¹

¹²¹ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 13.

In order for stability to be reached, these four conditions must be met, providing tangible indicators to assess the effect of Defend Forward. The thesis found that, from its implementation in 2018 until the present day in 2022, Defend Forward has had an indeterminant influence over the stability of the domain.

While indicators show that assured availability and integrity exist to a certain degree in the domain, an effect of Defend Forward on these conditions cannot be shown. The peaceful management of change in the cyberspace domain, as a requirement for stability, has certainly not been met. While international standards and agreements exist to manage change, a universal mechanism is absent, and stakeholders such as the PRC actively are seeking to develop their own standards.¹²² While this trend does not look promising for the development of stability, there is little evidence to suggest the Defend Forward is responsible for or has significantly influenced these developments from 2018 to 2022.

The final condition of stability is the absence of escalation from an initial level of tension. While there is no significant evidence of vertical or horizontal escalation in the cyberspace domain since 2018, there is also inconclusive evidence that Defend Forward has impacted this. In the short term, there is simply a lack of evidence directly tying Defend Forward to non-escalatory tension management in the cyberspace domain. When looking at the immediate effects Defend Forward had on the conditions for stability, it cannot be determined if Defend Forward had any significant impact on the stabilization or destabilization of the domain.

Due to the indeterminant results in analyzing the immediate effect of Defend Forward on the cyberspace domain, projecting out to assess the likely effects of Defend Forward in the long term was crucial. To accomplish this, Defend Forward was analyzed in relation to each of the eight cooperative norms that would result in a stable domain, as envisioned by the GCSC.¹²³ In every instance, judicious application of Defend Forward was assessed to likely support, or at the very least not detract from, the cooperative norms.

¹²² Park, “Breaking the Internet: China-U.S. Competition Over Technology Standards.”

¹²³ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 13.

Initially this appears to suggest that Defend Forward will positively influence the domain toward stability.

Despite Defend Forward supporting these eight norms, analysis of the structural characteristics of the cyberspace domain makes clear that reaching a goal of enduring stability in the cyberspace domain is likely impossible. Rapid evolution of technology, a culture of anonymity, and low barrier of entry will likely preclude stabilization in cyberspace. For this reason, Defend Forward likely does not move the cyberspace domain any closer to stability despite supporting the eight proposed norms. However, this is not to say that supporting the norms has no impact. These norms are generally positive developments for the cyberspace domain, and by implementing Defend Forward in such a way to support these norms, the United States gains legitimacy of its action on the international arena. This legitimacy helps to build relationships and cooperation, which when operating in a complex domain are greatly beneficial.

Overall Defend Forward does not make a significant impact on the stability of cyberspace, because cyberspace is an environment whose structural characteristics preclude stability. Notions that Defend Forward should seek to gain security through achieving stability are inherently flawed by equating the unreachable goal of stability with very reachable U.S. cyber security objectives. As such, emphasizing the development of stability over immediate security concerns can be detrimental to overall U.S. interests.

C. THE DEGREE TO WHICH PROMOTING STABILITY SUPPORTS U.S. INTERESTS IN THE CYBERSPACE DOMAIN

While aspiring to stability in the cyberspace domain is ultimately quixotic, as it is an unrealistic state in the domain, there are benefits to pursuing stability as part of a defense strategy like Defend Forward. The cooperative norms outlined by the GCSC largely do not contradict the security objectives of Defend Forward, and there are potential benefits to staying within the guardrails of acceptable behavior that these norms propose. However, security is and must be the ultimate objective. To lose sight of this would result in an ineffective strategy and lessen the security for U.S. interests in the cyberspace domain.

The promise of norms in international relations liberal theory is that stakeholders should and will adopt the norms because it will lead to a stable environment, which is an equilibrium state mutually beneficial to all parties.¹²⁴ As such, by adopting norms, a stakeholder shows their willingness to work toward this goal that benefits all parties. For this reason, Defend Forward generally maintaining its persistent engagement within the lines of the established or proposed norms can be beneficial.

Building relations and trust between stakeholders in the cyberspace domain is beneficial. Whether through bilateral or multilateral agreements, there is utility in working with partners in creating a more secure domain. What might be a threat to the security of U.S. interests might also be a threat to the security of United Kingdom or North Atlantic Treaty Organization interests. Therefore, building trust with likeminded partners in the domain through maintaining adherence to cooperative norms could have utility. If USCYBERCOM were to pursue persistent engagement to the maximum extent possible, disregarding ideal norms of behavior, the trust between potential partners could erode, and cooperation could become more difficult.

While adhering to norms may be beneficial, it must not trump pursuing security as the ultimate goal. While adhering to norms can build international legitimacy, it may also hamper USCYBERCOM from providing security to U.S. interests in cyberspace. An example of how this could work is the disclosure of vulnerabilities. The GCSC sets forth a norm that vulnerabilities should be systematically and transparently handled, and the default behavior should be disclosure.¹²⁵ This is a complicated model in terms of security. Whereas disclosure of some vulnerabilities discovered by USCYBERCOM can increase the security of systems vital to U.S. national interests, some disclosures would compromise USCYBERCOM's ability to create friction and dissuade malicious actors from threatening U.S. interests. To be effective, a balance must be found, and that balance would depend on the situation at hand. Thus, adhering to the norm, and defaulting to disclosure, would not necessarily be in the interest of U.S. security. Further, there is no guarantee that other

¹²⁴ Romaniak and Grice, "Norms, Norm Violations, and IR Theory," 2.

¹²⁵ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, 21.

stakeholders in the cyberspace domain would disclose these vulnerabilities, for the same reason. As there is little verifiable trust between stakeholders in the cyberspace domain, U.S. security would suffer if it blindly adhered to the norm.

Norms in cyberspace have a beneficial function for U.S. security. Norms do not serve to create stability, but rather serve as a means to build trust and positive relations with likeminded partners. Security should not be sacrificed to maintain a norm as those norms serve to support security and not vice versa. Defend Forward has great potential to increase the security of U.S. interests in cyberspace, and norms can assist in achieving this goal. However, the balance of security and norms should always tilt toward security.

D. RESEARCH LIMITATIONS AND FUTURE WORK

Studying a recently implemented strategy in a domain of constant evolution is a difficult process. As such, this thesis was restricted in the analysis that could be done. Over time, as Defend Forward moves past its initial years of operation, future study will be able to reveal less speculative effects of the strategy. However, as Defend Forward is still new and largely unproven in the domain, it is critical to assess the effects it has at this early juncture. Providing analysis to illuminate likely effective paths toward security is beneficial at this early stage.

1. Research Limitations

One limitation to this study is the cyberspace domain itself. As described earlier in this thesis, the cyberspace domain is in a state of constant and rapid evolution. This limits the accuracy of projecting long-term effects of Defend Forward. Unlike when USCYBERCOM implemented a deterrence strategy to counter the threats they expected, Defend Forward was implemented to counter threats that existed. While deterrence ultimately proved ineffective and Defend Forward is better aligned to provide security against existing threats, this may not always be true in the cyberspace domain. Cyberspace has evolved greatly since its early days of networked computers and predicting the evolution of the domain becomes more and more speculative as one looks further into the future. Thus, analysis done in 2022 will need to evolve with the domain to be relevant, and

more speculative conclusions drawn in this thesis may not be accurate if the domain evolves in a new direction.

While the conclusions reached regarding the immediate effects of Defend Forward are less speculative, they are restricted by limited data. Defend Forward was implemented four years prior to this writing, and as such determining trends in this short period is difficult. Conclusions drawn about trends in cyberspace attacks against U.S. interests since 2006 allow a greater understanding of overall trends of attacks against U.S. interests, as this longer period reduces the error in tracking events and trends. However, when specifically looking at the years since 2018 when Defend Forward was implemented there is not much data to eliminate error to the same degree. Thus, the conclusion that Defend Forward was likely somewhat effective at reducing the severity of attacks against U.S. interests cannot be made with a high level of certainty.

The dataset of cyber incidents from the Council on Foreign Relations that this thesis analyzed was limited to attacks from State or State affiliated sources. This limits the analysis of incidents to only a portion of the cyber incidents targeting U.S. interests. This was done from necessity as a comprehensive list of all attacks against U.S. interests would be an unmanageable amount of data. However, Defend Forward protects against threats from non-state actors, as well as state actors. Therefore, a likely significant portion of data was not included in this study. No accessible database exists with a comprehensive list of all cyber incidents targeting all U.S. interests from any possible source. However, if such a database existed, conclusions about the effects of Defend Forward could potentially be more conclusive.

This thesis used the definition of stability from the GCSC, which is not a binding or authoritative source of international law. As such the definition that the GCSC drafted is merely a proposal. Differing definitions of stability in the cyberspace domain can and do certainly exist. The GCSC definition was useful for this thesis, as it is not tied to a specific country or policy but is the product of a diverse international committee. However, it is also a very specific and very ambitious definition of stability. A more general definition could lead to differing conclusions as to how Defend Forward might affect the domain in regard to that specific definition of stability. However, the conclusion remains that

cyberspace is a rapidly evolving domain, with a low barrier to entry, and little trust. These conditions will likely make any definition of stability unattainable, despite potential support from U.S. cyber defense strategy.

2. Future Work

As Defend Forward is a recently implemented strategy there is still much research that needs to be done to understand Defend Forward's effectiveness, and the effects it will have on the cyberspace domain. As with all strategies, constant evaluation and analysis allows for course corrections, greater insight, and ultimately greater effectiveness.

Persistent engagement in the cyberspace domain to maximize security of U.S. interests is an ambitious goal. As such, a greater understanding of the feasibility of true persistent engagement is useful. At what threshold does a threat to U.S. interest warrant USCYBERCOM to engage to create friction? As the cyberspace domain is constantly evolving and threat vectors constantly evolve, how does USCYBERCOM best identify threats and create friction in such a way as to be proportional to the threat, while effective at disincentivizing attack? These questions would help to develop a methodology for assessing cyber threats and matching persistent engagement activity to threats, while keeping USCYBERCOM actions proportional and noncontradictory with legitimacy building norms.

Additionally, further study is needed to understand the effects Defend Forward has on the cyber policies and strategies of other stakeholders in the cyberspace domain. This will likely depend on the perceived effectiveness of Defend Forward, but U.S. allied and partner nations could build off of U.S. models of security for their own Defend Forward like strategies. How would multiple friendly Defend Forward like strategies operating in the same domain space effect the security of U.S. interests?

Alternatively, if U.S. competitor nations were to adopt a persistent engagement strategy, how would this affect the ability of Defend Forward to secure U.S. interests? A recent thought exercise conducted by Herb Lin, from the Center for International Security and Cooperation at Stanford University, supposes that China creates a Peoples Liberation

Army Cyber Command.¹²⁶ Building on the USCYBERCOM 2018 Command Vision, this exercise imagines the PRC adopting a persistent engagement model of defense to protect Chinese “cyber sovereignty” against the U.S. seeking “cyber hegemony”.¹²⁷ As Lin describes, this situation would produce competing Defend Forward strategies in the cyberspace domain. This in turn, could generate an environment of advocacy of rival norms: one pursued by the U.S. and one by the PRC. Each country would advocate their set of norms as most beneficial for their own security. It is unlikely the U.S. would accept the PRC using persistent engagement to set up their own system of norms as legitimate, much as the PRC today does not accept the U.S. defining norms in cyberspace as legitimate.¹²⁸ This hypothetical situation is not far-fetched, as the PRC views their “cyber sovereignty” as an essential element of their own national security.¹²⁹

Widespread adoption of Defend Forward like strategies by U.S. allies and adversaries alike could fundamentally alter the existing operating conditions of the cyberspace domain. Hence, the potential impact of such a system on U.S. security deserves future research. If persistent engagement proves as effective as this thesis concludes, a new paradigm in the cyberspace domain could take hold. Understanding the complex interactions of multiple stakeholders engaging in this type of strategy under this new paradigm will be needed.

¹²⁶ Herb Lin, “A Hypothetical Command Vision Statement for a Fictional PLA Cyber Command,” *Lawfare* (blog), October 22, 2021, <https://www.lawfareblog.com/hypothetical-command-vision-statement-fictional-pla-cyber-command>.

¹²⁷ Lin.

¹²⁸ Lin.

¹²⁹ Michael Kolton, “Interpreting China’s Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence,” *The Cyber Defense Review* 2, no. 1 (2017): 119–54, 120.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Assumpcao, Clara. "The Problem of Cyber Attribution Between States." E-International Relations. May 6, 2020. <https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/>.
- Brayton, Jenna. "The Seventh Summit of the Americas: The President's Trip and a Historic Meeting." whitehouse.gov. April 13, 2015. <https://obamawhitehouse.archives.gov/blog/2015/04/13/seventh-summit-americas-presidents-trip-and-historic-meeting>.
- Council on Foreign Relations. "Denial of Service Attacks against U.S. Banks in 2012–2013." Council on Foreign Relations. September 2012. <https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013>.
- . "Tracking State-Sponsored Cyberattacks Around the World." Council on Foreign Relations, Accessed April 10, 2022. <https://www.cfr.org/cyber-operations>.
- DeNisco Rayome, Alison. "Forrester's Top 6 Cybersecurity Predictions for 2018." TechRepublic. November 7, 2017. <https://www.techrepublic.com/article/forresters-top-6-cybersecurity-predictions-for-2018/>.
- Dobák, Imre. "Thoughts on the Evolution of National Security in Cyberspace." *Security and Defence Quarterly* 33, no. 1 (March 1, 2021): 75–85. <https://doi.org/10.35467/sdq/133154>.
- Fischerkeller, Michael P. and Richard Harknett. "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace." *Lawfare* (blog). November 9, 2018. <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>.
- Gaddis, John Lewis. "The Long Peace: Elements of Stability in the Postwar International System." *International Security* 10, no. 4 (1986): 99–142. <https://doi.org/10.2307/2538951>.
- Global Commission on the Stability of Cyberspace, *Call to Protect the Public Core of the Internet*, New Delhi: The Hague Centre for Strategic Studies, the EastWest Institute, 2017. <https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf>.
- . "GCSC Proposed Norms of Responsible Behavior in Cyberspace." Accessed April 30, 2022, <https://cyberstability.org/norms/>.

- . *Advancing Cyberstability*. New York NY: The Hague Centre for Strategic Studies, EastWest Institute, November 2019. https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf.
- . *Definition of the Public Core of the Internet*. Bratislava: The Hague Centre for Strategic Studies, EastWest Institute, May 2018. <https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf>.
- Goldman, Emily. “The Cyber Paradigm Shift.” In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 31–46. Newport RI: U.S. Naval War College Press, 2020. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>.
- Healey, Jason. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5, no. 1 (January 2019). <https://doi.org/10.1093/cybsec/tyz008>.
- International Security Advisory Board. *Report on A Framework for International Cyber Stability*. Washington, DC: U.S. Department of State, July 2, 2014.
- Internet Society. “Open Internet Standards.” Internet Society. Accessed April 10, 2022. <https://www.internetsociety.org/issues/open-internet-standards/>.
- Jeffre, Lynsey. “Why Ransomware Attacks Are on the Rise — and What Can Be Done to Stop Them.” PBS NewsHour. July 8, 2021. <https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them>.
- Kieninger, Stephan. “A Preponderance of Stability: Henry Kissinger’s Concern over the Dynamics of Ostpolitik.” *The Journal of Transatlantic Studies* 17, no. 1 (March 2019): 42–60. <http://dx.doi.org/10.1057/s42738-019-00003-3>.
- Klimburg, Alexander. “New Conditions and Constellations in Cyber.” *Cyber Stability Paper Series*. The Hague: The Hague Centre for Strategic Studies, 2021. <https://hcsc.nl/report/cyberstability-paper-series-new-conditions-and-constellations-in-cyber/>.
- Maness, Ryan, Brandon Valeriano, and Brandon Jensen. “The Dyadic Cyber Incident and Dispute Data, Version 1.5.” The Naval Postgraduate School. Accessed April 6, 2022. <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset>.
- Miller, James and Neal Pollard. “Persistent Engagement, Agreed Competition and Deterrence in Cyberspace.” *Lawfare* (blog). April 30, 2019. <https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace>.

- Nakasone, Paul M. and Michael Sulmeyer. "How to Compete in Cyberspace." *Foreign Affairs*. March 17, 2021. <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>.
- Nakasone, Paul M. "Introduction: A Cyber Force for Persistent Operations," In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 1–8. Newport RI: U.S. Naval War College Press, 2020. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>.
- Paris Call. "The Paris Call of the 12 November 2018." Accessed April 10, 2022. <https://pariscall.international/en/call>.
- Park, Joshua. "Breaking the Internet: China-U.S. Competition Over Technology Standards." *The Diplomat*. Accessed April 30, 2022. <https://thediplomat.com/2022/02/breaking-the-internet-china-us-competition-over-technology-standards/>.
- Raymond, Mark. "Confronting the Ubiquity of Norms in Cyberspace and Cyber Governance." *Lawfare* (blog). March 12, 2020. <https://www.lawfareblog.com/confronting-ubiquity-norms-cyberspace-and-cyber-governance>.
- Romaniak, Scott, and Francis Grice. "Norms, Norm Violations, and IR Theory." *E-International Relations* (blog). November 15, 2018. <https://www.e-ir.info/2018/11/15/norms-norm-violations-and-ir-theory/>.
- Rosenzweig, Paul. "Cybersecurity Predictions for 2018." *Lawfare* (blog). January 2, 2018. <https://www.lawfareblog.com/cybersecurity-predictions-2018>.
- Rovner, Joshua. "Cyber War as an Intelligence Contest." *War on the Rocks*. September 16, 2019. <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/>.
- Scroxtton, Alex. "Nation-State Cyber Attacks Double in Three Years." *ComputerWeekly.com*. Accessed April 10, 2022. <https://www.computerweekly.com/news/252499042/Nation-state-cyber-attacks-double-in-three-years>.
- Sechser, Todd S., Neil Narang, and Caitlin Talmadge. "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War." *Journal of Strategic Studies* 42, no. 6 (2019): 727–35. <https://doi.org/10.1080/01402390.2019.1626725>.
- Shannon, Vaughn. "International Norms and Foreign Policy," In *Oxford Research Encyclopedia of Politics*. Oxford UK: Oxford University Press, 2017. <https://doi.org/10.1093/acrefore/9780190228637.013.442>.

- Smeets, Max. "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection." *Intelligence and National Security* 35, no. 3 (April 15, 2020): 444–53. <https://doi.org/10.1080/02684527.2020.1729316>.
- . "What Is Absent From the U.S. Cyber Command 'Vision'." *Lawfare* (blog). May 3, 2018. <https://www.lawfareblog.com/what-absent-us-cyber-command-vision>.
- Smeets, Max and Herb Lin. "An Outcome Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward." *Lawfare* (blog). November 28, 2018. <https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward>.
- The Aspen Institute. "A National Cybersecurity Agenda for Resilient Digital Infrastructure." December 2, 2020. <https://www.aspeninstitute.org/longform/a-national-cybersecurity-agenda-for-resilient-digital-infrastructure/securing-the-internets-public-core/>.
- The Brainy Insights. "Cloud Storage Market to Reach USD 353.81 Billion and Exhibit at a CAGR of 24.48% from 2021 to 2028." GlobeNewswire. January 20, 2022. <https://www.globenewswire.com/news-release/2022/01/20/2369910/0/en/Cloud-Storage-Market-to-Rreach-USD-353-81-billion-and-Exhibit-at-a-CAGR-of-24-48-from-2021-to-2028-The-Brainy-Insights.html>.
- U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*. Fort Meade: U. S. Cyber Command, 2018. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.
- . "USCYBERCOM: Mission and Vision." Accessed April 30, 2022. <https://www.cybercom.mil/About/Mission-and-Vision/>.
- U.S. Department of Defense. *National Cyber Strategy*. Washington, DC: U.S. Department of Defense, 2018. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
- U.S. Department of Defense. *The DOD Cyber Strategy*. Washington, DC: U.S. Department of Defense, April 2015. <https://www.hsdl.org/?abstract&did=764848>.
- U.S. National Security Council. *The National Security Strategy of the United States of America*, Washington, DC: The White House, 2002. <https://georgewbush-whitehouse.archives.gov/nsc/nssall.html>.

- U. S. Senate. *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 Presidential Election, Volume 2: Russia's Use of Social Media with Additional Views*. Report 116-XX. Washington, DC: 116th Congress 1st Session, Accessed February 18, 2022. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.
- Trump, Donald. "Remarks by President Trump and Chairman Kim Jong Un in a 1:1 Conversation." U.S. Embassy & Consulate in Vietnam. February 28, 2019. <https://vn.usembassy.gov/20190227-remarks-president-trump-chairman-kim-11-conversation/>.
- Turton, William, Michael Riley, and Jennifer Jacobs. "Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom." Bloomberg. May 13, 2021. <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>.
- Vergun, David. "Cybercom's Partnership with NSA Helped Secure U.S. Elections." *U.S. Department of Defense News*. March 25, 2021. <https://www.defense.gov/News/News-Stories/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/>.
- Warner, Michael. "A Brief History of Cyber Conflict," In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 13–31. Newport RI: U.S. Naval War College Press, 2020. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>.
- Wohlforth, William C. "The Stability of a Unipolar World," *International Security* 24, no. 1 (1999): 5–41.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California