REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
08-01-2020	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE
Defending Forward in Cyberspace and the Case for Transparency

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Christophe, Jean-Paul (LCDR)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Defending forward in cyberspace must be not only a DoD responsibility, but the responsibility of citizens with US Government support. Truer security can be achieved by addressing the distinctly human elements of the cyber dilemma than by viewing it as solely a military and technical problem. Cyber conflict has not changed the nature of conflict, nor has it changed the nature of the human beings who carry it out. Pursuing the adversary through cyberspace may be a necessary aspect of defending forward, but the larger part of the solution lies in shaping the human element. The USG can encourage mechanisms of discourse, transparency, and public understanding on cyber issues. This will encourage the growth of norms and stigmas, which will help to shape and limit the growth of cyber conflict. One approach is the creation of a government-supported private sector council with a mission to declassify and share cyber-related information with the citizenry. Cyber conflict at its core is a human enterprise more than a technological challenge. When defending forward more fully reflects this truth, it will be a boon to both cybersecurity and the greater national security enterprise.

15. SUBJECT TERMS
Defending forward; Cyber; Cyber deterrence; Cyber operations; DOD; Department of Defense; CYBERCOM; USCYBERCOM

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

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

MASTER OF MILITARY STUDIES

TITLE: DEFENDING FORWARD IN CYBERSPACE AND THE CASE FOR TRANSPARENCY

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: LCDR JEAN-PAUL CHRISTOPHE, USN

AY 2019-20

Mentor and Oral Defense Committee Member: Matthew J. Flynn, Ph.D.

Approved:

Date: 20200428

Oral Defense Committee Member: Christopher S. Stowe, Ph.D.

Approved:

Date: 20200428

Executive Summary

Title: Defending Forward in Cyberspace and the Case for Transparency

Author: Lieutenant Commander Jean-Paul Christophe, United States Navy

Thesis: Defending forward in cyberspace must be not only a DoD responsibility, but the responsibility of citizens with US Government support. Truer security can be achieved by addressing the distinctly human elements of the cyber dilemma than by viewing it as solely a military and technical problem.

Discussion: The DoD's policy for defending forward in cyberspace is a sound approach that will likely produce some positive outcomes, but it is also only a piece of the cyber security puzzle. *Joint Publication 3-12 Cyber Operations* (JP 3-12) divides the cyber domain into three separate regions: blue cyberspace (friendly), red cyberspace (adversary), and gray cyberspace (other). To effectively defend forward, DoD cyber operators must freely traverse red and gray space. Sovereignty concerns are not as defined in cyberspace as in the physical world, but they should still be a consideration. However, JP 3-12 treats gray space as an unrestricted maneuver space for DoD cyber operations. There are potentially dangerous political consequences for this lack of regard, especially with respect to US partners. Therefore, more judicious policy needs to be crafted, and gray space redefined. Cyber conflict has not changed the nature of conflict, nor has it changed the nature of the human beings who carry it out. Pursuing the adversary through red and gray space may be a necessary aspect of defending forward, but the larger part of the solution lies in shaping the human element. The USG can encourage mechanisms of discourse, transparency, and public understanding on cyber issues. This will encourage the growth of norms and stigmas, which will help to shape and limit the growth of cyber conflict. One approach is the creation of a government-supported private sector council with a mission to declassify and share cyber-related information with the citizenry.

Conclusion: Cyber conflict at its core is a human enterprise more than a technological challenge. When defending forward more fully reflects this truth, it will be a boon to both cybersecurity and the greater national security enterprise.

DISCLAIMER

List of Tables

Page

Table of Contents

Defending Forward in Cyberspace

The United States Department of Defense (DoD) cyber strategy is to "defend forward," meaning that the protection of US infrastructure and interests in cyberspace requires offensive action beyond the Department of Defense Information Network (DoDIN) and US-owned networks. Because cyberspace is a medium that transcends state borders and negates physical distances, threats can come from anywhere around the globe. Due to this vulnerability, US forces must defend proactively by conducting intelligence, surveillance, and reconnaissance (ISR) outside of US network infrastructure and suppressing threats before they can penetrate friendly networks. In this way, defending forward is analogous to the US military's physical presence around the world: it maintains situational awareness and if necessary neutralizes threats to US interests long before they can actually threaten the homeland.[1] According to General Paul Nakasone, Commander, US Cyber Command (CYBERCOM), the DoD initially had a purely defensive cyber mission, reacting to threats as they presented themselves. However, as the volume of cyberattacks grew, the strategy had to evolve an offensive aspect to keep pace with the threat. Nakasone writes, "We must 'defend forward' in cyberspace, as we do in physical domains….[O]ur forces must operate against our enemies on their virtual territory as well. Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons..."[2] This is a sound argument, and defending forward in cyberspace is a sound approach. However, while it will likely produce some positive outcomes in the long run, it is still only a piece of the cyber security puzzle. Notwithstanding its highly technical nature, the day-to-day conflict in cyberspace is a human struggle fueled by human motivations.[3] This is to say that defending forward in cyberspace, even extremely aggressively, is still a reactive methodology that fails to address the underlying causes of malicious cyber

activity. An analogous construct in the physical world would be for US special forces to pursue perpetual tactical anti-terrorism engagements around the globe in the absence of a cohesive US Government (USG) strategy to undermine the root causes of terrorism. While the DoD will always have a tactical and operational role in protecting US and allied networks, the strategic key to limiting the deleterious effects of cyber conflict is to promote transparency and public understanding of the daily struggle in cyberspace. This will accelerate the speed at which this new and often intimidating domain is internationally normed and/or legislated into a more manageable challenge. Increased transparency will promote discourse between the governments of different nations, and between governments and their own citizens, which will force these issues into the consciousness of more than simply intelligence officers and technical experts. This will expose the potential ethical and legal quandaries innate to defending forward, for example the ambiguity of "trespassing" on partner nation (PN) networks as they are defined under the DoD's current conception of cyber "territory." When the mystique of cyberspace is lifted, and its daily machinations infused into the public psyche, the natural processes of discourse and behavioral modification that shape every human endeavor will take hold.[4] Defending forward in cyberspace must be not only a DoD responsibility, but the responsibility of citizens with wider USG support. Truer security can be achieved by addressing the distinctly human elements of the cyber dilemma than by viewing it as solely a military and technical problem.

This paper will investigate the nature of defending forward by assessing the DoD conception of cyberspace, its mission therein, and the problems associated with its approach. It will also examine the nature of cyber conflict and its similarity to all human conflict, demonstrating that a strictly military model for defending forward only partially addresses the

challenge. Finally, it will revise the DoD model of cyberspace and show how the USG can expand defending forward with public engagement and increased transparency. The author addresses these points within a conceptual framework built from scholarly sources and USG documents.

The Conflict in Cyberspace

Since its inception, the internet has grown rapidly from a network of physically-connected computers, switches, routers, and wires to a diverse community of interconnected devices communicating both with and without human involvement. This phenomenon is commonly referred to as the Internet of Things (IoT). In 2016, an estimated 9 billion devices were connected to the IoT, and researchers assess the total may grow to between 50 billion and 1 trillion devices by 2025.[5] It is now almost a prerequisite that everyday devices performing functions as old as the Industrial Revolution have some IoT capability so that a user can remotely monitor or manipulate them. IoT now encompasses an enormous swath of computers and devices from large and complex industrial control systems (ICS) to personal entertainment devices: electrical power distribution systems, hydroelectric dam controls, commercial and residential building thermostats, medical devices, smart televisions, fitness watches, and coffee makers are all apparatus that a legitimate user or cyber attacker can access with the right credentials. Additionally, the proliferation of electromagnetic spectrum communications technology has elevated the internet from a terrestrial and physically-defined network to an airwave-enabled grid riding on radio waves (this includes cellular), microwaves, and even light waves (laser) transmitted in the atmosphere and space.

As the number of devices grows, so too does the network's interconnectedness, complexity, functionality, and inevitably—vulnerability. In addition to the functionality it is

designed to provide, each device also presents a unique pathway to access other devices. Used honestly by the intended user, this is simply an additional access point. However, an access point viewed from a different perspective is a vulnerability or attack vector. As devices become "smarter" and their processes are increasingly automated by microchips and software, the potential errors in code or design that may provide surreptitious access are increasingly difficult to discover and correct. This is to say, a single device may actually contain multiple attack vectors. For example, a typical smartphone runs on a complex operating system (iOS, Android), receives and transmits in multiple ways (cellular, Wi-Fi, Bluetooth, GPS), and contains multiple pieces of third-party software (Uber, Google Maps, Angry Birds); each of these capabilities or applications likely has multiple oversights (or even malicious intentional vulnerabilities) that if discovered can be exploited to produce effects limited only by a cyberattacker's skill and imagination. By extension, the more that basic societal functions (electrical distribution, water treatment, building security) grow to depend on IoT, the more that the basic operations of society may be nefariously disrupted by one of these vulnerabilities. There is a virtual goldmine of attack vectors available to malign actors who seek to exploit the system, whatever their motives; they need only devote the time to finding the inevitable oversights.

Malicious actors come in a variety of forms. The traditional tale of the hacker as a lone operator writing computer viruses in his basement for the simple pleasure of sowing anarchy and chaos has expanded into a more complex story. Hackers now comprise loose organizations of geographically displaced technology-savvy individuals with activist agendas (hacktivists), criminal individuals and syndicates, and states conducting espionage and military operations through explicitly or tacitly sanctioned organizations.[6] Additionally, black market operators sell software tools and sets of remotely-controllable victim computers (botnets), providing the raw

material to fuel even more illicit activities. On the opposing side are private cyber security companies, benign state military cyber operators, private and state cyber intelligence organizations, and even benevolent associations of individuals defending internet freedom. While every cyber interaction is a unique and fluid event, many traditional tensions of conflict and tenets of warfare exist even in the virtual world. Actors will attempt to probe adversary or target networks for vulnerabilities and access opportunities, then surveil the network for ways to cripple it, extract information, or cause it to do something consistent with their goals. The defending side is attempting to find and repair its own vulnerabilities (patch), defeat incoming probes, eliminate breaches, and, if possible, anticipate and disable incoming attacks. Anticipating and disabling attacks at their source is the crux of defending forward.

The expansion of malicious cyber actors and proliferation of cheap and simple exploitation tools has substantially lowered the barriers of entry to harass users through cyberspace. Small states and non-state actors can create effects and wield cyber power at low cost when compared to the expense to compete in the sea, air, and space domains.[7] In fact, states and organizations that can afford the most cyber capability likely also have the most vulnerabilities.[8]

While there is still a large gap between the random disorganized actions of individuals employing simple tools they purchased or downloaded (“script kiddies”) and the coordinated cyber campaigns of state cyber operations, the costs to business and government to defend against them are nonetheless palpable. For example, the Council of Economic Advisers estimates that nefarious cyber action cost the US economy between $57 billion and $109 billion in 2016.[9] These facts converge into a simple truth: the sheer amount of malicious cyber activity and the ever-changing landscape create an eternal struggle with no real end but definite advantages for

the offense. After all, the offense need only succeed once to gain access, and it will continue to evolve new ways to do it as new attack vectors enter the grid.[10] Additionally, the adage "a threat to one is a threat to all" holds particularly true in cyberspace. The most conscientious and well-organized cyber defense may be rendered moot by the poor habits of other companies with which it does business. In 2013, hackers exfiltrated the credit card data of 40 million customers from Target Corporation by exploiting a vulnerability in the network of a third-party heating and air conditioning contractor that serviced some of its stores.[11] This illustrates the necessity for governance and coordination, but also provides the rationale for defending forward. The concept of defending forward is built on the realization that sitting back on US networks attempting to deflect a constant blitz of evolving tools and techniques across a shifting attack surface is at best no better than treading water, but by sheer probability bound to fail eventually. Instead, the DoD has devised a strategy to move to the sources of these attacks, conduct I&W to provide decision space and notification for decision makers, and if necessary disable these activities. As former US Deputy Secretary of Defense William Lynn writes, "The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun. Cyberwarfare is like maneuver warfare, in that speed and agility matter most. To stay ahead of its pursuers, the United States must constantly adjust…".[12]

Blue Space, Red Space, and Gray Space

Joint Publication 3-12 Cyber Operations (JP 3-12) divides the cyber domain into three separate regions: blue cyberspace, red cyberspace, and gray cyberspace. It defines these spaces in the following:

> The term "blue cyberspace" denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the…(DODIN), cyberspace forces prepare, on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the US and PNs [partner nations]. The term "red cyberspace" refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.[13]

(For simplicity, the three brands of cyberspace will be referred to as just "blue space," "red space," and "gray space" hereafter). JP 3-12 names CYBERCOM the DoD coordinating authority for cyber operations, with the responsibility to "prepare to, and when directed, conduct military CO [cyber operations] external to the DODIN, including in gray and red cyberspace, in support of national objectives."[14] The objectives of defending forward are defined by this phrase. The core strategy, essentially, is to operate to the maximum extent possible in gray and red space in order to prevent an adversary from marshalling his capabilities and attacking blue space.

To effectively defend forward, DoD cyber operators must freely traverse red and gray space to build situational awareness. Activities may include but are not limited to: monitoring attack and intrusion attempts, searching for malware that could be used in future attacks, analyzing foreign network vulnerabilities, and monitoring adversary behavioral patterns to more accurately predict future attacks. DoD cyber operators must keep a constant watch on red and gray space such that the adversary has nowhere to hide—no bastion from which to safely plan malicious activities against blue space. In short, defending forward is a variation of the old adage "the best defense is a good offense." It aims to disrupt the adversary's ability to project mischief into blue space from his own backyard (red space), as well as to deny him the ability to expand his backyard through the acquisition and incorporation of gray space. The concept is simple and elegant *a priori*, but unfortunately may lead to troubling behavior when executed utilizing the

DoD's current definitions of blue, red, and gray space. To clarify these issues, it is necessary to construct a crosswalk of friendly, adversarial, and third-party actions and presence in cyberspace and examine the logical implications (see Table 1).

Table 1: Cyberspace according to JP 3-12 definitions

		1	**2**	**3**
		Adversary Controlled	Partner Controlled	Third-Party Controlled
A	Adversary Owned	RED	RED	RED
B	Partner Owned (protect agreement)	RED	BLUE	RED
C	Partner Owned (no protect agreement)	RED	GRAY	GRAY
D	Third-Party Owned	RED	N/A	GRAY

Table 1 demonstrates the logical outcomes of JP 3-12's definitions. The easiest space to define is gray, as it is everything left after designating blue space and red space. Next, red space is everything either owned or controlled by an adversary. Another way to look at this is any space that the adversary can freely use to his advantage. It may include infrastructure that he has built himself or contracted to have built, as well as infrastructure that once belonged to another of which he has wrested control through coercive cyber operations. In Table 1, all of row A and column 1 is thus red space. This includes cells A2 and A3, which are owned by the adversary but have been seized by a US partner and a third-party, respectively. It is still a useful construct for the DoD to regard A2 and A3 as red space, as the adversary will likely make efforts to reacquire them and may utilize them again in the near future to threaten US interests.

The formulation of blue space is slightly more complicated and will present an important dilemma. To simplify all tables, a column and row for US ownership and control have been omitted. US space is blue by definition, unless seized by an outside party, at which point it will be red until returned to US control. This goes for both public and private US infrastructure, as the DoD may be ordered to protect both. (The intricacies of how and under what conditions it should intervene on behalf of private US infrastructure is a policy issue that will be explored later, but as to the question of whether it should lend assistance if requested, the answer is decidedly in the affirmative). After putting aside US infrastructure, what remains as potential blue space is partner infrastructure, i.e. the cyberspace owned and/or controlled by friendly and allied states (PN's).

This definition needs to be taken a step farther, however, as the mere fact of residing or belonging to a PN does not imply blue space. This is to say that where PN's are concerned, blue spaces include only "areas DOD may be ordered to protect,"[15] not simply spaces under the auspices of the PN. This is a vital distinction, as it is important to consider that cyber operations are inherently invasive. In contrast, red space is defined by its relation to acknowledged USG adversaries or actors that have inflicted coercive cyber operations upon US infrastructure and therefore must be regarded as bad cyber actors. Thus, operations in red space are already part of cyber conflict. The same cannot be said for operations across PN infrastructure. It would be questionable behavior indeed for the DoD to conduct cyber operations on any PN infrastructure that has not been added to the blue space inventory. In practical terms, addition to blue space inventory entails an official agreement with the PN government stating that it desires DoD protection, *and upon which network infrastructure it desires it.* This is an explicit as opposed to implicit action. For this reason, Table 1 contains 2 rows for PN infrastructure; row B denotes

partner infrastructure with an arrangement for DoD protection, whereas row C represents all other partner infrastructure. This means that the DoD can only act with impunity in Row B. Row C should be treated as the property of a foreign sovereign or foreign citizens. It can either be red or gray space, but not blue.

Thus, row C is the focal point of a moral dilemma (see Table 2). Should the DoD become aware of adversary operations in PN non-agreement space, it faces a quandary regarding how to respond. Even worse, what should the DoD do if a PN non-agreement network is commandeered by the adversary, thus turning it into red space by the JP 3-12 definition? What if the adversary is using that network as a foothold from which to threaten blue space? The tenets of defending forward specify that the DoD should intervene and neutralize the threat, but the ethics of the situation demand that it stay clear of PN infrastructure it has not been authorized to enter. This is where JP 3-12 definitions of red, blue, and gray space become problematic. A palpable tension exists between the dictates of the mission, which encourage unhampered traversal of red and gray space, and the expectations of a partnership, which dictate that one ought to respect the boundaries the other party has established. The potential damage to US credibility for failing to respect this boundary can cause long-term damage to current partnerships and impair the ability to create new ones. The areas where DoD operations could be ethically questionable are represented in Table 2 by crosshatching. These areas are PN non-agreement infrastructure plus cell D1, which denotes a third-party's infrastructure that has been seized by an adversary. While D1-type infrastructure will not be further explored in this paper, it should be noted that it must be red space by the JP 3-12 definition, but occupying it without permission in order to fight the adversary could have similar implications for US credibility.

Table 2: Cyberspace with crosshatching where DoD operations are ethically questionable

		1	2	3
		Adversary Controlled	Partner Controlled	Third-Party Controlled
A	Adversary Owned	RED	RED	RED
B	Partner Owned (protect agreement)	RED	BLUE	RED
C	Partner Owned (no protect agreement)	RED	GRAY	GRAY
D	Third-Party Owned	RED	N/A	GRAY

Everything that has not already been designated red or blue is left to gray space. Also of note, cell D2 holds a peculiar permutation: third-party-owned but partner-controlled infrastructure. This circumstance is sufficiently exceptional as to be inapplicable to this conversation and is marked as such. Having completed an investigation of the logical outcomes of the JP 3-12 definitions for blue, red, and gray space, it is now fitting to examine the consequences in a real-world context.

Cyberspace and Sovereignty

The JP 3-12 definitions of blue, red, and gray space provide a serviceable if problematic model upon which the DoD has built its concept of cyber operations. It posits an essentially Westphalian view of cyberspace, the implications of which should be familiar to a US military audience. For example, from the perspective of a US cyber operator addressing an adversary, the designations “blue,” “red,” and “gray” correspond to “mine,” “yours,” and “neutral or ungoverned,” respectively. The very fact that blue space exists to defend means that the US must recognize a partition in cyberspace, a border where sovereign US “territory” begins. When bad

actors cross or attempt to cross this line, the US considers it unacceptable and employs DoD operators to expel or repel the invaders. The same process occurs in the physical world with state borders and actual military forces. JP 3-12 models cyberspace in the same Westphalian tradition in order to build a foundation for defending forward. However, it seems to sidestep or ignore some of the potential consequences. Cyberspace may be fluid, but it is not without borders, and it cannot be completely divorced from awareness of state sovereignty.[16]

Patrick Franzese advances a compelling argument about why state sovereignty must be a consideration in cyberspace. First, cyberspace lives on physical infrastructure that is located within traditional borders. This infrastructure must be owned and administered by individuals, organizations, or governments, all of which have state affiliations of some kind. Second, inter-state commerce in cyberspace is still subject to the laws of the states involved; internet commerce would be free-for-all if not for this fact. Third, the information that traverses cyberspace still affects and holds value in the physical world. Take for example, intellectual property stolen from a US firm by a Chinese hacker, or as Franzese mentions, the proliferation of child pornography on the internet by miscreants. While these bytes of information may be flowing freely through cyberspace, they still shape reality for the involved parties beyond cyberspace, whether entrepreneurs or exploited minors. "No 'cyberspace exemption' shields information from the valid interests of the state where information is sent, received, or stored."[17] Since states promote their interests in the physical world, by definition they must defend those interests in the cyber world or suffer real world consequences. Finally, state-owned critical infrastructure is now accessible through cyberspace, meaning that the physical well-being of the state depends in part on cyber defense.

Demchak and Dombrowski further argue that Stephen Krasner's classical indicators of Westphalian sovereignty are all emergent properties of cyberspace. The four primary qualities are territoriality, autonomy, control, and mutual recognition.[18] Cyberspace exhibits territoriality and autonomy when states apply their laws to cyberspace infrastructure and the people using it, and, most importantly, by the fact that these acts go uncontested by other states. An example is the US decision to make the possession of child pornography on its networks illegal. Territoriality is a geographic quality, expressing dominion over some infrastructure but not others; autonomy, while closely related in this case, denotes an exclusivity in applying that law on certain networks that other states do not dispute. Control corresponds to the act of policing certain cyberspace, regulating who crosses into it, and monopolizing coercive force within it. This certainly exists by stint of the entire conversation on defending blue space. Finally, mutual recognition implies that other states accept that a state carries out the other three functions on certain infrastructure, *and acknowledge its authority to do so*.[19] This certainly occurs in modern cyberspace. Thus, despite the liberal and democratizing influences that have shaped cyberspace, it would be a grave mistake to completely ignore sovereignty issues in planning and conducting cyber operations.

Cyberspace and Physical Space

In the physical world, borders divide the earth into states controlled by sovereign governments. State authorities (law enforcement, border patrol, military) enforce and protect these borders from within and without; they work together to ensure that no external party can cross these borders without the government's authorization. The exact point at which fixed borders and respect for sovereignty became customary is debatable, but the Peace of Westphalia in 1648 is an acceptable approximation. Since then, the practice has been reinforced with

countless agreements and treaties, as well as norming and legislative actions by multilateral organizations like the United Nations (UN). The 1958 Convention on the High Seas and later the 1982 United Nations Convention on the Law of the Sea (UNCLOS) were treaties that further advanced the concept of physical sovereignty, now including the oceans and airspace. States were allotted a twelve nautical mile strip of water, measured from the coastline or continental shelf as applicable, to augment their sovereign territory; these territorial waters could be policed and administered exclusively by the owning state just like land within state borders. Similarly, all airspace within state borders or above territorial waters was equally exclusive and dubbed territorial airspace. All other waters and airspace were held in common by all states: a state could neither claim nor deny them to others.[20] Naturally, many states dispute the extent of the territorial waters allotted to them for various reasons. Some claim that twelve nautical miles is an arbitrary distance that should vary with the size of the state, while others simply take issue with the way that their twelve nautical miles were surveyed. Despite disagreements over specific details, the international community generally accepts the premise that states should have land borders, some measure of exclusive water and airspace, and that the remaining spaces should be designated the commons.

A practical illustration of these ideas will build clarity: in this example, the fictitious US Navy destroyer *USS Ownship* will conduct a maritime patrol during peacetime. *Ownship* represents the entire fleet in this example, so it will receive no specific tasking other than to freely roam the oceans, build situational awareness for the US Navy, and promote US security through vigilance and armed presence as necessary. The idea is much like defending forward.

After putting to sea from Naval Base San Diego, *Ownship* may first spend a few weeks patrolling the US coast. As a US Navy asset, it is authorized to navigate freely inside UNCLOS-

defined territorial waters that extend from the coast out to twelve nautical miles. It can also make port calls in US ports like Alameda, California and Kitsap, Washington as required. By analogy, territorial waters are blue cyberspace, and *Ownship* is a CYBERCOM or other DoD operator defending US networks (although not defending forward as yet). Along the way, *Ownship* will challenge any vessel it encounters that is inside of US territorial waters without proper authorization. If the unauthorized vessel is of US registry or is otherwise non-military, *Ownship* will take any immediate actions necessary to defend the coastline but will promptly contact the US Coast Guard to handle the incident as a law enforcement matter. This distinction is worth emphasizing: while the DoD must certainly take action to protect US infrastructure from imminent danger, it cannot prosecute US persons and is not ideal for handling foreign criminals and/or civilians. Those duties fall within the purview of the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS). This raises issues about cyber defense that will be addressed later. On the other hand, if *Ownship* encounters a foreign warship called *Attacker* in US territorial waters, it will impede *Attacker* and, in accordance with UNCLOS and US Navy rules of engagement, use violence if necessary to stop the ship's advance. Conversely, *Attacker* violates nothing by sailing at 12.5 or even 12.1 nautical miles from the US coast. In such a case, prudence demands that *Ownship* would follow and attempt to ascertain its intentions, but *Attacker* is in international waters and may not be interfered with simply for being near a US coast.

After its jaunt in US territorial waters, *Ownship* may proceed out to sea to continue its patrol. Once it is farther than twelve nautical miles from the US coast (and not closer than twelve nautical miles to the Canadian or Mexican coasts) *Ownship* is in international waters. By UNCLOS, these waters are held in common by all states. *Ownship* may not restrict the freedom

of navigation of a foreign ship nor may it be restricted by any foreign ship in these waters. It is also important to note that *Ownship* is now defending forward, by patrolling and watching for threats beyond US waters; in the cyber analogy it is operating beyond blue space to protect US interests. *Ownship* will likely spend the majority of its patrol time here in international waters, showing presence and US resolve, and monitoring for any signs that a foreign ship intends harm to the US homeland. If *Ownship* should glean such an intention, or if it is furnished the appropriate intelligence from another source, *Ownship* can more effectively protect here than closer to the US coast. Ostensibly, international waters are the equivalent of gray cyberspace, but this analogy will be shown problematic later.

Ownship may not cross into any but US territorial waters without authorization from the owning state. If it does, it should expect to be challenged or attacked by that state's naval authorities. While the USG may order *Ownship* to do this in a special case where it is absolutely essential to national security, such action is provocative and escalatory and should not be taken lightly. The cyber equivalent is defending forward by entering red (adversary-owned or controlled) cyberspace.

Ownship must also avoid the territorial waters of even friendly nations. The mere fact of an alliance does not automatically grant access, for example, to Australian territorial waters, unless such access was explicitly conferred by the alliance treaty. Although *Ownship* would probably not be attacked for entering Australian waters without authorization, the action would neither be appreciated by the Australian Government (AG). This would not lead to war but would be indicative of a callousness antithetical to the concept of partnership. In the next scenario, if the AG has granted the US unfettered access to only some of its territorial waters, *Ownship* must take care to transit only those. For example, the AG may allow *Ownship* access to

Moreton Bay to facilitate a port visit to nearby Brisbane, but this does not mean *Ownship* may of its own volition also visit Botany Bay south of Sydney. Access to a specific area does not imply access to all areas. Similarly, if *Ownship* has an embarked helicopter, AG authorization to enter Botany Bay does not mean that the helicopter can overfly Sydney without a separate authorization. In short, there will almost always be areas that the AG chooses to share and others that it does not. In Tables 1 and 2, this is the difference between cells B2 and C2, respectively. Cell B2 signifies partner-owned space that has been explicitly shared with the DoD for the purposes of combined cyber operations, making it blue space. Cell C2 represents space which is partner-owned but has not been shared, which makes it gray space by the JP 3-12 definition. Thus, it is problematic that defending forward treats all gray space as homogenous and unrestricted to cyber operations. The same movement restrictions that apply to *Ownship* when sailing near Australia ought to limit DoD freedom of action near partner-owned cyberspace.

Recommendation: Redefining Gray Space

It should be apparent by this point that the similarities between physical space and cyberspace falter at gray space. For sure, US territory and partner-owned territory that the US has been permitted to access are like blue space. Also, an adversary's territory and areas that it has illegally seized are like red space. It would seem that the final step is equating international waters and airspace, the commons, to gray space. However, this is inaccurate. The reason is that cyberspace is entirely constructed by humans; there is no naturally-occurring or unclaimed cyberspace. Every piece of infrastructure, every switch, and every cellular tower was connected by an individual, an organization, or a government. Everything belongs to someone. If this is the case, then there is truly no gray space where the DoD can defend forward without trespassing on someone else's infrastructure.

On a certain level, this is an arbitrary statement, though. Precious few can actually access the internet independently: most connect through chartered or rented infrastructure provided by telecommunications companies. Additionally, surfing to any given website may involve traversing nodes in several different countries, and the average user has little control over the path his computer takes to the destination. If this is the case, should there be such a thing as blue space and red space? Should everything be considered one homogeneous interdependent gray space held in common by all? Cerf, Ryan, and Senges address this idea, stating "While the Internet is a physical artifact with components in many countries, the virtual space created by that artifact is defined by logical boundaries rather than geophysical borders."[21] The authors go on to argue that internet governance through treaties will never work because of this peculiarity, so instead behavior should be normed through consortiums of experts and concerned parties with minimal involvement by governments. Admittedly, this argument holds merit, but it naively ignores certain aspects of human nature. While cyberspace cannot be physically partitioned as readily as land, sea, and sky, neither can it exist as an indivisible whole evenly shared by all parties. As mentioned in the previous section, information in cyberspace has consequences in the physical world (laws, commerce, etc.), so state sovereignty concerns can never be entirely eliminated from the equation. Second, to the extent that an organization invests labor and capital to build cyber infrastructure, human nature demands some say in what occurs on it. A cyber commons in the truest sense will never exist. However, neither will true cyber sovereignty in the Westphalian sense.

Nonetheless, JP 3-12 treats gray space as though it were a cyber commons, an unrestricted maneuver space for DoD cyber operations. This lack of regard poses two risks. In the case of unshared partner networks, it may alienate friends. Alternatively, in the case of gray

space owned by a third-party, it may create an adversary from a previously disinterested state (Tables 1 and 2, cell D3). Finally, some may argue that because cyberspace is an interconnected network of mutually dependent components, any user of it tacitly agrees to become a node in service to the network. For example, in its journey to a particular website, an individual's computer may traverse multiple countries in a fraction of a second. The argument continues that if this is the case, the DoD is doing nothing different than the average individual by freely traversing gray space. Unfortunately, this argument suffers from a misinterpretation of scale and intent. It is true that most individuals and organizations do not find it objectionable that their infrastructure is routinely used as part of a system designed to promote communication, research, entertainment, and commerce—the original intent for cyberspace and the internet. It is politically untenable and potentially self-defeating to suppose that they would feel the same about hosting sanctioned military and intelligence operations by the USG.

A comprehensive solution to this dilemma will require further study and assessment of military operational necessity versus political risk. Subsequent actions will need to weigh the national security value of operating on a given piece of gray cyberspace, the states affected by that operation, and an assessment of USG goals with respect to them. This goes beyond the scope of this paper. However, one immediate recommendation is to amend the JP 3-12 definition of gray space to reflect Table 3. In Table 3, all partner infrastructure without a protection agreement receives a special designation: yellow cyberspace. Similarly all third-party infrastructure (excepting the odd case of cell D2) should receive the same designation. Gray space is thus eliminated, and defending forward must be reevaluated with considerably less unrestricted space.

Table 3: Cyberspace with proposed yellow space

		1	2	3
		Adversary Controlled	Partner Controlled	Third-Party Controlled
A	Adversary Owned	RED	RED	RED
B	Partner Owned (protect agreement)	RED	BLUE	RED
C	Partner Owned (no protect agreement)	YELLOW	YELLOW	YELLOW
D	Third-Party Owned	YELLOW	N/A	YELLOW

This proposal will necessarily convert from red to yellow any cyberspace controlled by an adversary but either owned by a partner (without a sharing agreement) or a third-party, as in cells C1 and D1. While these spaces were previously designated red due to adversary actions, they deserve to be treated with some sensitivity due to their actual ownership. Overall, the introduction of yellow space and elimination of gray space supports the hypothesis that it is unsustainable and ultimately self-defeating to treat current gray space with the same restrictions as the cyber infrastructure of acknowledged adversaries. Such actions will alienate allies and create new adversaries. Converting these potentially sensitive spaces to yellow acknowledges a need to craft more judicious policy for operating within them.

The Limits of Defending Forward

Evidence up to this point has shown that the conflict in cyberspace is carried out on a daily basis by myriad actors. Entities that threaten US interests include nefarious individuals of both political and apolitical agendas, individual criminals and syndicates, and militaries and intelligence apparatus. Any of these activities may also be sponsored, incentivized, or tacitly

encouraged by state governments. The parties involved shape an ongoing power struggle: each side surveys the capabilities and weaknesses of the adversary, attempts to exfiltrate sensitive information, tries to alter and manipulate the other's infrastructure, and strives to influence the opponent's decision-making process while preserving his own options. This should sound eerily familiar even to the cyber-uninitiated, because in essence it describes the history of human conflict and competition. The DoD crafted the strategy of defending forward in order to cope with this highly dynamic environment, but defending forward is a military approach to a broader conflict, not a solution.

The majority of the nefarious activity in cyberspace should not be characterized as warfare. Lucas Kello provides a useful framework that divides cyber activity into three categories: cybercrime, cyber exploitation, and cyberattack. In his conception, cybercrime is the use of a computer to conduct an action already illegal under existing laws, for example financial fraud or the transfer of child pornography. Cyber exploitation is the use of computer systems to pilfer proprietary information or data, a tactic employed to great effect by the Chinese government and its proxies against the US defense industrial base (DIB). Finally, he notes that the purpose of a cyberattack is to cause damage, whether virtual damage to the operation of a network or physical damage to the industrial infrastructure it controls. The former could be a distributed denial of service attack (DDOS) against the email server at an electrical company; attackers would flood the computer with enough email to crash the operating system, thereby reducing the productivity of the office. In the latter case, attackers might compromise a computer that actually controls electrical transmission, thereby causing physical damage to actual components of the municipal power grid; this is known as a cross-domain attack because it emanates from cyberspace but causes tangible effects in the physical world. Lastly, Kello writes

that a cross-domain attack that "produce[s] significant physical destruction or loss of life"[22] should be designated cyberwar, but that only a tiny percentage of cyberattacks meet this benchmark.[23] This last point is particularly important when considering the role of the DoD.

Thomas Rid goes so far as to suggest that cyberwar does not and likely will never exist. Using a classical Clausewitzian definition of war, he argues that war must be the application of actual violence by a known actor to achieve stated political ends.[24] In his estimation, the nature of the cyber domain most likely precludes a true cyberwar from ever occurring. For example, cyber effects are generally not violent, and in select cases where physical damage has been wrought, either the act was unattributed or cyber was not the sole means toward a political end. In some ways this is a semantic argument: Rid still believes that cyberattacks can be cause for legitimate concern, just that they will never be an independent means of waging war.[25] He writes, "[T]he last decade saw increasingly sophisticated acts of network-enabled sabotage, espionage, and subversion….But the question is if a trend is leading to inevitable acts of stand-alone cyber war, with code as the main weapon, not as an auxiliary tool that is nice to have."[26] Both Rid and Kello agree, however, that cyber aggression does not by definition constitute warfare. It is instead an expression of age-old human tendencies. Where Kello sees cybercrime, cyber exploitation, and cyberattack, Rid sees either entirely apolitical cybercrimes or politically-motivated sabotage, espionage, and subversion.[27]

Thus, across the range of nefarious cyber endeavors, a very small portion, if any, actually constitutes war. This should certainly draw into question the role of the DoD in preventing and curbing these activities. The prosecution of cybercrime is a law enforcement activity, an undertaking more fit for the FBI or DHS. Cyber exploitation goes hand-in-hand with espionage and grand larceny; the lead authority is merely a question of the identity of the perpetrator

(individual or state) and the national security implications of the stolen information. This mission belongs in part to the FBI and in part to national intelligence agencies. Sabotage and subversion are essentially the same action, where the targets are objects or human minds, respectively.[28] Sabotage may fall under DoD purview, depending on the target, but often it more closely resembles crime. Countering subversion is solidly a law enforcement or intelligence mission. To wit, mankind has wrestled with these challenges, now cyber-challenges, since the beginning of social history, and no amount of defending, forward or otherwise, will prevent them.[29] In almost all of these examples, the DoD may play a role, but should not take lead.

There are two natural counterarguments to this assertion. The first is that the FBI has no capacity to prosecute and defend against cybercrime and cyber exploitation. The second is that the DoD must defend forward to disrupt and deter attacks against national defense systems and critical infrastructure as part of its duty. These arguments are actually both valid. The FBI is already swamped with casework, counterintelligence, and enforcement duties in the traditional world, let alone the cyber realm. It stands to reason that an organization such as the DoD, with its vast resources in equipment and manpower, should stand-in to assist. As long as due regard is paid to *posse comitatus* such that the military does not target US persons, it is not harmful for the DoD to employ its cyber machinery to help curb cybercrime and cyber exploitation. The second argument also stands up. The DoD does in fact have the duty to protect national security in cyberspace, so it will always have a role in the strategic defense of DoDIN and key infrastructure, virtual or otherwise. The point that both of these arguments bear out, however, is that the cyber threat is a multi-faceted challenge more complex than “seek and destroy” or “find, fix, finish.” Defending forward is a piece of the equation, but not the entire solution; a major portion of the

solution lies beyond the cyber realm. Cyber conflict is, after all, a human problem enabled by technology, not the other way around.

Throughout history, no new tool or weapon has fundamentally altered the nature of human conflict. The technology used in warfare and human competition has only shifted the efficiency, lethality, and effects by which human beings impose their wills on one and other. The same is true in cyberspace. Cyber conflict has not changed the nature of conflict, nor has it changed the nature of the human beings who carry it out. It follows that the solution for minimizing the harmful effects will fall to a great extent outside of the cyber realm. However, this concept is the opposite defending forward in its current form. Kello writes that, regrettably, "the analysis of cybersecurity has effectively been ceded to the technologists. Consequently, public perceptions of the cyber issue display…a propensity to think of 'cyber threats' as pernicious lines of code—instead of focusing on the human agents who utilize them, and their motives for doing so."[30] These threats exist insofar as there are conflicting human interests and potential profits, so the issue should be examined from a different angle. This is to say, pursuing the adversary through red and gray space may be a necessary aspect of defending forward, but the larger part of the solution lies in shaping the human element.

Recommendation: Expanding the Concept of Defending Forward

The international conflict in cyberspace operates largely out of the view of the public; this is due both to its esoteric nature and the deliberate efforts of governments to classify their efforts. Consequently, much of the necessary discourse associated with this domain has been left to technical experts, intelligence officers, and the minority of politicians with the security clearance and political imperative to pay attention. This problem must be addressed in order to stimulate the process of normalizing cyber conflict.

Cyber conflict continues to evolve and expand largely out of the public eye for predictable reasons. First, cyberspace is a relatively new technology, and any technology in its infancy is typically mysterious to the average consumer. Cyberspace has the added hurdles of being highly technical in design and highly conceptual in nature. While one can see the physical infrastructure that enables it to function, cyberspace itself exists beyond the physical realm so familiar to human beings. Mathematics, physics, and electricity have not changed, but the near exclusivity with which they govern cyberspace is jarring to most individuals. Additionally, the internet in its current form is still so new that the majority of the workforce and national leadership did not come of age using it. The result is a lack of top-down political will to force this technology and its implications out of the shadows and more fully integrate it with the public discourse. To wit, governments should play a large role in developing this aspect of defending forward.

According to N.J. Ryan, there are several methods of stabilizing and regulating the conflict in cyberspace; among them are "norms," "taboos," and "association."[31] In the spirit of examining defending forward from a more holistic and human perspective, norms, taboos, and association are particularly useful. All three are very similar in that they recognize the powerful behavior-shaping mechanisms of collective human consciousness. This is to say, the more that people recognize and address a problem, the quicker methodologies and solutions are born. However, this also means that these methodologies depend on transparency and public participation. Ryan defines norms as "non-binding conventions or a standard of appropriate behaviour about how a class of actors should act."[32] Taboos yield similar results through negative reinforcement: they "refer to the inappropriate ways of acting or cultural mores that are 'off-limits'."[33] Finally, association is the public coupling of cyber identities and real-world

identities, connecting cyber actors to real world people and organizations. This activity is often referred to as "naming and shaming" because it destroys cyber anonymity. The association methodology can also spotlight governments that tacitly and explicitly enable nefarious actors. Rid and Buchanan argue that, while attribution and association in cyberspace may be resource intensive, success is more a function of political will than technical constraints. In other words, if the political stakes are high enough, a state with moderate cyber capability will find a way to name and shame its attacker to within a reasonable probability. This is particularly the case for an entity with the resources of the USG.[34] It is equally irrelevant to argue that malign actors can work in secret without alerting the authorities of the state in which they are operating. In such cases, it is sufficient for the victim to identify the state from which the activity originated, then request its help in eliminating the problem. If the "hosting" state refuses to cooperate, then the victim is free to associate it with the perpetrators.

Mazanec and Shamai examine norms and taboos for cyber activity by drawing upon mankind's history with weapons of mass destruction. They argue that the main reason states adopt norms regarding the utilization of new weapons is self-interest. The state must be forced into a position wherein the unrestricted use of the weapon creates more problems than advantages.[35] To a certain extent, the utterly devastating potential of nuclear weapons was self-norming; the existential threat their employment posed to mankind ensured that no government made plans to use them except in the direst of emergencies. With the potential extinction of mankind on the table, an intensely practical ban on the use of nuclear weapons matured alongside the technology. On the other hand, cyber conflict, while serious, has not risen to a level where most people regard it as an existential threat. It likely will not, except in narrow instances where cyber effects interact with nuclear command and control mechanisms. Nonetheless, these

cases are too specific to norm cyber conflict out of existence. The use of chemical weapons may provide a better example than nuclear weapons. Chemical weapons became the face of human carnage after World War I, and an international stigma developed so utterly that most states were not willing to weather the storm of reprisal and ostracism associated with their further use.[36] A collective conscience and consciousness tabooed the employment of chemical weapons and largely eliminated their widespread use. Mazanec and Shamai reason that encouraging these same mechanisms, whether under the banner of a taboo or stigma, can help to shape and limit the growth of cyber conflict.[37] The USG can facilitate this process by encouraging discourse, transparency, and understanding on cyber issues. Stigmas, taboos, and eventually norms develop when regular people form opinions, but regular people do not form opinions about issues they rarely see and do not understand.

Lastly, the overclassification of cyber operations is both a cause and symptom of the public's lack of understanding of cyber conflict. As mentioned previously, it is natural for new technology to be viewed with some trepidation. It is also an all too familiar phenomenon for a government to use varying levels of confidentiality to jealously guard new technology, particularly once it has been weaponized. This secrecy banishes the nuances and implications of that technology to the shadows, where the innately human processes of consideration, approval, and aversion cannot reach it. Instead, the discourse falls in the hands of technocrats, bureaucrats, the intelligence community, and the military. Overclassification is self-perpetuating in that it often arises when practitioners do not understand a subject matter well enough to fastidiously delineate the elements that need to be protected. Consequently, large swaths of information that should become common knowledge for the edification of all remain hidden. This preserves the lack of understanding. Such is the case with cyber conflict in the US, and the propensity to view

defending forward as a uniquely military affair. Assuredly there is much that must be kept under wraps due to operational realities and national security, but far too much remains completely out of view of the average citizen.

Relegation of cyber conflict to the classified realm results in both a decrease in the rate at which norms develop and a lack of sincere self-reflection and consequence evaluation that arise from public involvement. Conversely, greater transparency will lead to long-term benefits in international partnership as well as participation from the US populace. The government has a role both in the education of the people and the policy which will help to shape norms. Defending forward will ultimately be more successful with the assistance of these mechanisms. The final issue becomes the creation of a framework the USG can utilize to achieve these ends.

Recommendation: The Cyber Transparency Council

Crucial to the goal of promoting cyber transparency is the creation of a board of cyber experts charged with forging the link between government, industry, and the citizenry through policy recommendations, classified information review, and information dissemination. To simplify discussion, this body will be referred to as the Cyber Transparency Council (CTC). The CTC must be USG-funded and safeguarded, yet primarily staffed and managed by private sector individuals. It must not be placed under the auspices of the DoD or in any way tied to US defense budgeting. It is likely best positioned under executive or congressional sponsorship; to provide some insulation from continuous partisan push and pull, consideration should be given to incorporating the council as a long-term presidential task force.

The CTC must substantially represent private sector interests and viewpoints, particularly those of the technology and media industries. The former will provide subject matter expertise and business perspective, while the latter can offer technical expertise, a critical eye, and a

relentless partiality for the public's "need-to-know." By nature, both industries will aggressively pursue constructive solutions for chronicling cyber activity, showing it to the public, and facilitating increased cooperation between the public and private sectors. In fact, each stands to gain privately from enabling this process. Other CTC representatives could hail from non-governmental organizations, private sector intelligence, insurance, law, and cyber-vulnerable heavy industries. All selected individuals must be eligible for security clearance; this will maximize their utility as reviewers and ultimately facilitators of declassification. Private sector seats on the council must substantially outnumber government seats for this reason especially. It is imperative that the CTC have a strong bias for declassification and communication with the public. It is, however, unrealistic to expect that the council will have its own disclosure authority, as this responsibility will always reside with the originator (except when delegated for narrowly-defined and standard tasks). Notwithstanding, if appropriately championed by an influential sponsor such as the Executive Branch, the council can shift the classification paradigm to one in which the originating agency must show why information needs to remain under lock and key rather than the opposite. Another potential outcome is that the CTC may force originators to more precisely define the classified aspects in a body of information, which will yield benefits far beyond this conversation when it becomes standard practice. Finally, the CTC should also have members from the DoD, government intelligence community, and executive, legislative, and judicial branches as required. Again, government representatives must remain in the strictly enforced minority. At a later stage, strong consideration should also be given to expanding the CTC to include industry equivalents from partner nations. The precise number of individuals, nomination procedures, selection process, term lengths, and voting dynamics is a matter for a different study on organizational principles and processes. Insofar as the council reflects certain

key principles, the administrative details can vary. These principles include: a strong ratio of private sector the government individuals, ardent support from an influential governmental USG entity, a broad representation of industry with an emphasis on media and technology, and a predisposition to disseminate information widely.

The council's mission is simple but vital: to democratize thought with regard to the current cyber conflict by sharing as much information as possible with the citizenry. This will promote discourse, understanding, and enable the generation of cyber norms and stigmas. The CTC should utilize all manner of dissemination: a website, periodicals, social media, and any other mediums that emerge. Subject matter of particular interest may include cyber intelligence and threats, government and industry cyber operations, best practices and sensible advice for average users, and current events to include spotlighting bad cyber actors. The more the public learns, the more it will develop expectations, impressions, and stigmas. The collective consciousness will gradually expand. In this, the CTC members themselves will possess a prophet-like mission, having been given the rare opportunity to glimpse a world few can, and directly responsible for bringing their fellow citizens to a comparable level of understanding. It is, however, important to emphasize that the council is not fueled by the altruistic nature of its members; such a construct would be too precarious. The council constituents hail from civilian industries who stand to gain from inducing the USG to be more transparent about cyber conflict. Heavy industry and the technology sector will benefit from the increased understanding of previously classified cyber incidents, while the media industry will doubtless want to disclose and report as much as possible. Thus, while looking out for themselves these members will in fact be looking out for their fellow citizens as well.

The council's second objective is to further integrate private industry into the mission of defending forward. The board will, by its composition, create a natural forum for critically examining the practices that can empower the private sector and alleviate the burden on the government cyber security apparatus. The blueprint for this approach actually already exists, although the implementation is not ideal. The 2018 Cyber Information Security Act (CISA) created an agency under DHS for the express purpose of disseminating cyber security information and working with the private sector to secure critical US infrastructure. However, the agency falls short for two reasons. First, as it belongs to DHS, its mission will always be security first and foremost with all other considerations being ancillary. This means that its mission is to protect, not to inform and innovate. Second, its focus is critical infrastructure, which means that it is boresighted on the elite organizations within the private sector whose operations are deemed essential to national security. This is quite different from a council designed to inform and look out for the interests of the common user. The presence of foreign representatives on the CTC will also provide a venue to address the privacy concerns associated with the DoD's problematic framing of blue, red, and gray cyberspace. The same mechanisms working to declassify and demystify cyber operations for the US public will also facilitate an atmosphere of transparency with PN's. The CTC should scrutinize the legal and privacy concerns associated with gray and proposed yellow space, as well as explore more precise ways to define them. A civilian body championed by government, the CTC provides an opportunity to broaden defending forward from a military discourse to a human discourse. The council goals, while US-focused, with time will shape the international cyber arena by impacting the way the DoD interacts with blue, red, and gray, and perhaps yellow space. As defending forward is

designed to protect national security, this approach will address the challenge more comprehensively.

Conclusion

This paper has shown that defending forward, as currently defined by the DoD, is a useful but incomplete approach to promoting US security in cyberspace. When cyber conflict is viewed as a strictly military problem of defending blue space, attacking red space, and utilizing gray space, the logical implications are troubling and strategically unsound for the United States. However, it should not be a surprise that the DoD would approach cyber conflict as an issue of borders, maneuver, and seizing and holding territory. Defending forward is essentially the cyber version of the DoD's approach to battle in the physical world, and what is cyber conflict if not an extension of traditional human conflict with new tools?

The conflict in cyberspace continues to expand as new devices are added to the IoT and more attack vectors are available to exploit. Individuals, criminals, and governments race to discover new vulnerabilities in software and hardware that will allow them to access and manipulate the cyber infrastructure of their victims and competitors. Victories are fleeting in this constantly shifting landscape, but hardly inconsequential. The costs of protecting against a never-ending stream of nefarious activities is immense, and technologically-advanced countries such as the United States are most vulnerable. In cyberspace, barriers to entry are low, and offensive actors have the advantage. Defending forward was designed to promote security by adding an offensive component to the US cyber strategy so that the DoD can prevent bad actors from threatening US interests outside rather than inside of US networks.

However, the division of cyberspace into blue, red, and gray by JP 3-12 has been shown problematic. Where blue is friendly-owned, red is adversary-owned, and gray is everything else,

there is potential for political disaster in gray space. By its definition, gray space includes the private networks of partner nations that they may not wish to share. Gray space may also include the infrastructure of countries that bear no ill-will toward the United States but may change their minds when used as a stepping stone. A more prudent approach is to reconfigure the DoD model of cyberspace, designating politically sensitive cyberspace as yellow and encouraging further study of the operational necessities and sociopolitical implications. While cyberspace has no physical borders, it cannot be completely divorced from claims of sovereignty. The information that rides on it has real world implications, so states will continue to exercise their authority and defend their interests in cyberspace. For these reasons the DoD needs to more carefully consider the implications of how it conducts cyber operations.

Cyber conflict has been shown to be more complex than a technical battle for the possession of virtual terrain. It is a continuation of a human struggle for knowledge of one's adversary and mastery over his decision-making process. The conflict in cyberspace more closely resembles a social struggle replete with espionage, criminality, and subversion than a technological battle between armies. For this reason, defending forward should be expanded to encompass a distinctly human element that can address these sources at their root. The DoD is often not the best candidate for the mission, as aspects of the conflict fall under law enforcement and wider government auspices. Through broader thinking, the USG can enable mechanisms that will increase cyber security not through the force of technology, but the latent potential of collective human engagement. Increasing the transparency of cyber operations and facilitating public understanding will accelerate the process by which the cyber dilemma is normed. One possible approach is the creation of a government-funded council primarily staffed by private

sector individuals. This council could represent the interests of the public and, if properly championed, transform the air of secrecy shrouding cyberspace and defending forward.

Cyber conflict at its core is thus a human enterprise more than a technological challenge. Just as every army joins battle under the weight of political realities, defending forward must also be fashioned around political implications. While DoD may own the operation, the larger strategy falls to the USG to shape the sociopolitical environment that has given rise to and perpetuates cyber conflict. While one cannot permanently change human motivations and behaviors, an appreciation for their preeminence does provide an advantage. If red cyberspace is where the adversary resides, then red cyberspace must be minimized. If blue cyberspace is where friends and allies reside, then it must be maximized. The surest path toward these goals is the judicious use of resources, whether it is the power of public opinion or the knowledge of where and where not to tread. When defending forward more fully reflects these truths, it will be a boon to both cybersecurity and the greater national security enterprise.

Endnotes

[1] US Department of Defense, *Summary of the Department of Defense Cyber Strategy*, (Washington, DC: Office of the Secretary of Defense, 2018), 2.
[2] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *JFQ: Joint Forces Quarterly*, No. 92 (2019 1st Quarter): 12.
[3] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security 38,* no. 2 (Fall 2013): 16.
[4] Brian M. Mazanec and Patricia Shamai, "Stigmatizing Cyber War: Mission Impossible?," in *2016 International Conference on Cyber Conflict* (Washington, DC: October 2016), 4.
[5] Sean S. Costigan and Gustav Lindstrom, "Policy and the Internet of Things," *Connections 15*, no. 2 (Spring 2016): 10. https://www.jstor.org/stable/10.2307/26326436
[6] US Cyberspace Solarium Commission, *March 2020 Report* (Washington, DC: Government Printing Office, March 2020), 17- 19.
[7] William J. Lynn III, "Defending a New Domain," *Foreign Affairs 89,* No. 5 (September 2010): no page number provided. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=52957873&site=ehost-live
[8] Joseph S. Nye, Jr., *The Future of Power: Its Changing Nature and Use in the Twenty-First Century* (New York: PublicAffairs, 2011), 124-125.
[9] Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Washington, DC: Executive Office of the President of the United States, February 2018), 36. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[10] Lynn, "Defending a New Domain," no page number provided. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=52957873&site=ehost-live
[11] Nicole Perlroth, "Heat System Called Door to Target for Hackers," *NYTimes.com*, February 5, 2014. https://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html
[12] Lynn, "Defending a New Domain," no page number provided. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=52957873&site=ehost-live
[13] Joint Chiefs of Staff, *Cyberspace Operations, Joint Publication 3-12* (Washington, DC: Joint Chiefs of Staff, June 8, 2018), I-4, I-5.
[14] Joint Chiefs of Staff, *Cyberspace Operations*, III-5.
[15] Joint Chiefs of Staff, *Cyberspace Operations*, I-4, I-5.
[16] Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist?" *Air Force Law Review* 64, (June 2009): 11-14. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=a9h&AN=45162330&site=ehost-live
[17] Franzese, "Sovereignty in Cyberspace," 13.
[18] Stephen D. Krasner, "Rethinking the Sovereign State Model," *Review of International Studies* 27, No. 5 (December 2001): 17-42. doi:http://dx.doi.org.lomc.idm.oclc.org/10.1017/S0260210501008014. https://search-proquest-com.lomc.idm.oclc.org/docview/204961312?accountid=14746

[19] Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs* (2013): 30-32. https://search-proquest-com.lomc.idm.oclc.org/docview/2228678154?accountid=14746
[20] "United Nations Convention on the Law of the Sea," December 10, 1982, 27. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
[21] Vinton G. Cerf, Patrick Spaulding Ryan, and Max Senges, "Internet Governance Is Our Shared Responsibility," *I/S: A Journal of Law and Policy for the Information Society,* 10, No. 1 (2014): 3. https://ssrn.com/abstract=2309772
[22] Kello, "Meaning of the Cyber Revolution," 20.
[23] Kello, "Meaning of the Cyber Revolution," 20. Kello notes that a similar definition is found in Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, No. 4 (Winter 2011): 21.
[24] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies,* 35, No. 1 (October 2011): 7-8.
[25] Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, No. 2 (Fall 2014): 181-192.
Lindsay uses elements of this argument as well, stating that physical violence is the only true form of warfare, while cyber capabilities can never rise to the level of Clausewitzian imposition of political will.
[26] Rid, "Cyber War Will Not Take Place," 29.
[27] Rid, "Cyber War Will Not Take Place," 7.
[28] Rid, "Cyber War Will Not Take Place," 16, 22.
[29] Rid, "Cyber War Will Not Take Place," 16.
[30] Kello, "Meaning of the Cyber Revolution," 16.
[31] N.J. Ryan, "Five Kinds of Cyber Deterrence," *Philosophy & Technology, 31*, No. 3 (September 2018): 331. doi:http://dx.doi.org.lomc.idm.oclc.org/10.1007/s13347-016-0251-1. https://search-proquest-com.lomc.idm.oclc.org/docview/2092368248?accountid=14746
[32] N.J. Ryan, "Five Kinds of Cyber Deterrence," 335.
[33] N.J. Ryan, "Five Kinds of Cyber Deterrence," 335.
[34] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies,* 38, 1-2 (December 2014): 7, 30-31, 33.
[35] Mazanec and Shamai, "Stigmatizing Cyber War," 1, 4.
[36] Mazanec and Shamai, "Stigmatizing Cyber War," 4.
[37] Mazanec and Shamai, "Stigmatizing Cyber War," 8.

Bibliography

Cerf, Vinton G., Patrick Spaulding Ryan, and Max Senges. “Internet Governance Is Our Shared Responsibility.” *I/S: A Journal of Law and Policy for the Information Society* 10, No. 1 (2014): 1-41. https://ssrn.com/abstract=2309772

Costigan, Sean S., and Gustav Lindstrom. “Policy and the Internet of Things.” *Connections,* 15, No. 2 (Spring 2016): 9-18. https://www.jstor.org/stable/10.2307/26326436

Demchak, Chris, and Peter Dombrowski. "Cyber Westphalia: Asserting State Prerogatives in Cyberspace." *Georgetown Journal of International Affairs* (2013): 29-38. https://search-proquest-com.lomc.idm.oclc.org/docview/2228678154?accountid=14746

Franzese, Patrick W. “Sovereignty in Cyberspace: Can It Exist?” *Air Force Law Review,* 64, (June 2009): 1-42. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=a9h&AN=45162330&site=ehost-live

Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security,* 38, no. 2 (Fall 2013): 7-40.

Krasner, Stephen D. "Rethinking the Sovereign State Model." *Review of International Studies* 27, No. 5 (December 2001): 17-42. doi:http://dx.doi.org.lomc.idm.oclc.org/10.1017/S0260210501008014. https://search-proquest-com.lomc.idm.oclc.org/docview/204961312?accountid=14746

Lindsay, Jon R. and Lucas Kello. “Correspondence: A Cyber Disagreement.” *International Security* 39, No. 2 (Fall 2014): 181-192.

Lynn, William J., III. “Defending a New Domain.” *Foreign Affairs,* 89, No. 5 (September 2010), 97–108. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=52957873&site=ehost-live

Mazanec, Brian M., and Patricia Shamai. “Stigmatizing Cyber War: Mission Impossible?” In *2016 International Conference on Cyber Conflict*. Washington, DC, October 2016.

Nakasone, Paul M. “A Cyber Force for Persistent Operations.” *JFQ: Joint Forces Quarterly*, No. 92 (2019 1st Quarter): 10-14.

Nye, Joseph S., Jr. *The Future of Power: Its Changing Nature and Use in the Twenty-First Century*. New York: PublicAffairs, 2011.

Nye, Joseph S., Jr. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly,* 5, No. 4 (Winter 2011): 18-38. https://search-proquest-com.lomc.idm.oclc.org/docview/1242014564?accountid=14746

Perlroth, Nicole. “Heat System Called Door to Target for Hackers.” *NYTimes.com*, February 5, 2014. https://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies,* 35, No. 1 (October 2011): 5-32. DOI: 10.1080/01402390.2011.608939

Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies,* 38, 1-2 (December 2014): 4-37.

Ryan, N.J. “Five Kinds of Cyber Deterrence.” *Philosophy & Technology*, 31, No. 3 (September 2018), 331-338. http://dx.doi.org.lomc.idm.oclc.org/10.1007/s13347-016-0251-1. https://search-proquest-com.lomc.idm.oclc.org/docview/2092368248?accountid=14746

“United Nations Convention on the Law of the Sea.” December 10, 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United States Council of Economic Advisers. *The Cost of Malicious Cyber Activity to the U.S. Economy*. Washington, DC: Executive Office of the President of the United States, February 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

United States Cyberspace Solarium Commission. *March 2020 Report*. Washington, DC: Government Printing Office, March 2020.

United States Department of Defense. *Summary: Department of Defense Cyber Strategy*. Washington, DC: Office of the Secretary of Defense, 2018.

United States Joint Chiefs of Staff. *Cyberspace Operations, Joint Publication 3-12*. Washington, DC: Joint Chiefs of Staff, June 8, 2018.