REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/15/2020	Master's Thesis	Aug 2019 - May 2020

4. TITLE AND SUBTITLE
CYBERSPACE AS OPERATIONAL ART: A COMMON POINT OF DEPARTURE

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
RONNIE B. YOUNG, Lt Col, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd.
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES
Not for Commercial Use without the express written permission of the author.

14. ABSTRACT
The term "cyber" is everywhere, from popular culture to discussions on national security. However, despite the term's prevalence, a common understanding of it remains elusive. This lack of a common understanding is even more pronounced when the discussion extends to cyberspace as an operational domain. The pervasiveness of cyberspace in the operational environment demands a deeper understanding of the operational implications of cyberspace. Through discussions on war and warfare in cyberspace, the nature and character of cyberspace, and the implications cyberspace holds for the operational design, this thesis offers a foundation on which to build the operational artist's understanding of cyberspace as an operational domain.

15. SUBJECT TERMS
Authorities, Center of Gravity, Competition, Cyber, Cyberspace, Cyberspace Threats, Decisive Points, Doctrine, Globalization, Gray Zone, Great Power Competition, Internet, Joint Function, Operational Art, Operational Artist, Operational Design, Operational Environment, War, Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			RONNIE B. YOUNG, Lt Col, USAF
UNCLASS	UNCLASS	UNCLASS	Unclassified Unlimited	66	19b. TELEPHONE NUMBER *(Include area code)* 757-443-6301

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATE COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33315-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report. e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

CYBERSPACE AS OPERATIONAL ART:

A COMMON POINT OF DEPARTURE

by

Ronnie B. Young

Lieutenant Colonel, United States Air Force

THIS PAGE INITIALLY LEFT BLANK

CYBERSPACE AS OPERATIONAL ART: A COMMON POINT OF DEPARTURE

By

Ronnie B. Young

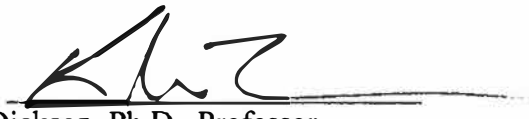
Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: 

15 MAY 2020

Thesis Advisor: Signature: 
Keith Dickson, Ph.D., Professor
Colonel (Ret), U.S. Army

Approved by: Signature: 
James Fosbrink, COL, U.S. Army
Committee Member

Signature: 
Miguel L. Peko, Captain, U.S. Navy
Director, Joint Advanced Warfighting School

THIS PAGE INITIALLY LEFT BLANK

Abstract

The term “cyber” is everywhere, from popular culture to discussions on national security. However, despite the term’s prevalence, a common understanding of it remains elusive. Understanding “cyber” as a term is difficult and becomes even more so when used as an adjective for other terms such as “effects”, “space”, “power”, and “war”.

It is not uncommon to hear the term “cyber” used with any number of varied definitions, intents, and outcomes. The varied use of the term, and mixed results of attempts to leverage cyber, make it clear that, without context or common understanding, the concept of cyber itself leads to confusion and misdirection. This difficulty in understanding cyber is even more pronounced when the discussion extends to cyberspace as an operational domain. The pervasiveness of cyberspace in the operational environment, and the Department of Defense’s increasing reliance on the cyberspace domain to conduct operations in support of national objectives, demands a deeper understanding of the cyberspace domain as it relates to military operations and the operational level of war. Therefore, it is essential to develop a greater understanding of the strategic and operational implications of cyberspace as a warfighting domain. Effectively employing cyberspace power requires not only a common understanding of what constitutes cyberspace power, but also a sophisticated understanding of cyberspace as an operational domain, and its relationship to the complementary operational domains of air, land, sea, and space. Through discussions on war and warfare in cyberspace, the nature and character of cyberspace, and the implications cyberspace holds for the operational design, this paper establishes a foundation on which to build the operational artist’s understanding of cyberspace as an operational domain.

Dedication

Though the work represented by these pages can in no way rival the contributions of those that made them possible, I dedicate this thesis to my bride, my children, my parents, and all who have borne the colors of our nation or carried the torch of freedom.

To my bride, thank you. Your perspective and feedback were invaluable to the development and refinement of this work. I will never be able to repay you for the patience and support you provided me during this endeavor, and over our 19 years as husband and wife. You are an amazing woman, wife, mother, officer, and friend. Serving alongside you and sharing a life with you have been two of the greatest honors of my life. You are my hero.

To my children, thank you. To my oldest son, I am proud of the man you have become. To my youngest son and my daughter, your positive attitudes and resiliency are an inspiration. You were a captive audience during the development and refinement of my thesis, and I am sure you heard more about the complexities of cyberspace than you would have preferred, but you listened without complaint. I am so proud of both of you.

To my parents, thank you. I would not be where I am today were it not for your love and support.

Acknowledgements

I would like to thank my thesis advisor, Dr. Keith Dickson, for his time, patience, support, and guidance. His perspective was instrumental to the development and direction of this work. I am in his debt.

I would also like to thank the faculty and students of Seminar One. The Professional Military Education experience can be a joy or a chore, and the greatest factor that influences which category the experience falls into is more often than not determined by the qualities and attitudes of those individuals sharing the experience. I count myself fortunate to have shared this experience with such a fine lot of dedicated professionals. I am grateful for their support, understanding, patience, and perspectives. My experience has been enriched by them.

Finally, I would like to thank my church family. Their support and encouragement these last 10 months have been a blessing to me and my family during this challenging time. I am forever grateful.

THIS PAGE INITIALLY LEFT BLANK

Table of Contents

Table of Figures

INTRODUCTION

In early 2017, a meeting was held in one of the many small, non-descript conference rooms scattered across the National Capital Region[1] to discuss plans and operations for one of the many Joint Task Forces (JTF) active at the time.[2] The team included representatives from the JTF's operations and planning elements, Department of Defense organizations, and inter-agency partners. The JTF representatives described their mission and the strategic ends toward which the JTF was working. At a point in the discussions, the lead operations planner for the JTF indicated that cyber was being considered as a means by which the JTF could achieve the desired strategic end-state. This generated numerous questions, as nearly everyone in attendance expressed an opinion on what cyber meant.

When pressed to clarify what they meant by cyber, the JTF representatives did not answer the question specifically, but only added another layer of confusion by stating that the goal would be to generate cyber effects. This response met with even more questions, as well as concerns, about the potential unintended consequences of the ways and means of the JTF's plans. Questions asking for details concerning the cyber elements of the JTF's plan created only more confusion and frustration among the attendees. As a result, the meeting ended without resolution.

---

[1] The National Capital Region (NCR) is recognized as the District of Columbia and portions of Maryland, extending north to Fort Meade, east to Joint Base Andrews and Northern Virginia, south to Marine Base Quantico, and west to Dulles International Airport.

[2] The Joint Task Force is a joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander when the scope, complexity, or other factors require capabilities of multiple Services or Military Departments operating under a single commander. Joint Task Forces vary in size and scope based on the requirements and the conditions driving their establishment. Office of the Joint Chiefs of Staff, *Joint Task Force Headquarters,* Joint Publication 3-33, (Washington, D.C.: The Joint Staff, 31 January 2018).

As the above vignette illustrates, "cyber" is a difficult term and becomes even more so when used as an adjective for other terms such as "effects", "space", "power", and "war". It is not uncommon to hear the term "cyber" used with any number of varied definitions, intents, and outcomes. From a commander without any understanding simply directing the integration of cyber into operations, to a task force operations officer making a vague request for cyber effects, it is clear that, without context or common understanding, the concept of cyber itself leads to confusion and misdirection. This difficulty in understanding cyber is even more pronounced when the discussion extends to cyberspace as an operational domain.[3]

The misunderstanding surrounding cyberspace as an operational domain, however, is not the first time that the emergence of a concept or operational domain has confused and misdirected military leaders. Following World War I, with aerial units having proven their relevance in combat, airpower advocates such as Brigadier General William "Billy" Mitchell lobbied heavily to advance the cause of air power. Mitchell even went so far as to suggest that the airplane and the submarine would render the traditional surface navies of the world, to include the United States Navy, irrelevant to future war.[4] Mitchell was the most prominent officer who spoke out in favor of developing air as an operational domain and as a key aspect of future war. Mitchell faced

---

[3] The terms "cyber" and "cyberspace" are often used interchangeably in contemporary conversations on the subject. This tendency contributes to confusion on the subject and perpetuates misunderstanding among those charged with developing strategy and operational concepts for activities that leverage and/or rely on the domain. In this paper, the author uses the term "cyber" as a reference to discussions or specific concepts promulgated in contemporary literature and conversation on the subject. The replacement of the term "cyber" with the term "cyberspace" is intentional, and serves to clarify understanding by avoiding the nebulous concept of cyber, as using the term "cyber" alone provides neither clarity nor context.

[4] Gregory J. Rattray, *Strategic Warfare in Cyberspace*, (Massachusetts: Massachusetts Institute of Technology, 2001), pp. 235-247.

the same confusion and frustration that many officers today face in their proponency of cyber as an operational domain.

The most impassioned discussions related to cyber and cyberspace to this point have focused on the areas of cyber security, cyber defense, and cyber crime. The sheer volume of available literature on, and the growth of an entire industry related to, these three areas reveals a very narrow appreciation for the domain.[5] Through the lenses of cyber security, cyber defense, and cyber crime, cyber is perceived only in terms of the threat to existing systems. The subjects of cyberspace security, cyberspace defense, and cyberspace crime have received the vast majority of attention over the past three decades. While these areas are certainly relevant to discussions on cyberspace, and contribute greatly to the larger body of knowledge on the subject, this paper focuses on an area of cyberspace discussion that has been largely overshadowed by cyberspace security, cyberspace defense, and cyberspace crime—cyberspace as an operational and warfighting domain.[6]

Beyond cyberspace security and defense, there are ongoing debates and discussions related to the fundamental make up of cyberspace, the nature of cyberspace, and the role cyberspace plays in the contemporary global strategic environment. What is driving these debates and discussions is the realization that cyberspace, regardless of the

---

[5] The global market value for the industry was $112.01 billion in 2019. Fortune Business Insights, "Cyber Market Size, Share & Industry Analysis, 2019 – 2026," Fortunebusinessinsights.com, February 2020, under "cybersecurity market analysis-2026," (report ID: FBI101165) https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 (accessed March 15, 2020).

[6] To illustrate, a recent *Google Scholar* search for publications discussing cyber security, cyber defense, and cyber crime provided a cumulative total of 1,498,000 publications related to the topics. Compare this to the 7,540 cumulative returns for a similar *Google Scholar* search for publication related to cyberspace as a domain (accessed November 14, 2019).

lens through which one views it, has fundamentally altered the interactions between states, between states and individuals, and between individuals themselves.

While the definition of cyberspace itself is widely accepted, other cyber-related definitions vary greatly depending on the descriptor associated with the term. For example, Dennis Poindexter indicated that more than 35 definitions for "cyber war" existed at the time of his 2015 book, *The New Cyberwar*. Poindexter himself defined cyber war as the "part of war that incorporates both the control and the use of information to influence the will of the people, not limited to the parties of the dispute."[7] The term "cyber war", however, is not present in any Department of Defense publications.[8]

While the Department of Defense has recognized the importance of the cyberspace domain, it has not taken a comprehensive approach to make this domain operationally effective; this must happen in order to bring strategic and tactical actions into a coherent whole.[9] The 2018 Department of Defense Cyber Strategy states that "leaders and their staffs need to be 'cyber fluent' so they . . . are positioned to identify opportunities to leverage the cyberspace domain to gain strategic, operational, and tactical advantages."[10] The central problem is that cyberspace is misunderstood as an

---

[7] Dennis F. Poindexter, *The New Cyberwar: Technology and the Redefinition of Warfare*, (North Carolina: McFarland & Company, 2015), p. 5.

[8] The author's search was limited to publicly-available documents (strategy, guidance memoranda, and doctrine) and does not include any classified documents or training materials specific to cyber-related specialties within the Department of Defense.

[9] The Department of Defense has—on a limited basis—applied cyberspace capabilities in coordination with activities in other domains (see Secretary of Defense Ash Carter's "cyber bombs" statements); however, available literature on the subject suggests that these instances of inclusion of cyberspace capabilities in cross-domain operations were more likely the result of an "add on" approach rather than a deliberate, pre-planned integration of cyberspace capabilities at the operational level of war.

[10] U.S. Department of Defense, Office of the Secretary of Defense, *2018 Department of Defense Cyber Strategy*, (Washington, D.C., 2018), p. 5.

operational domain due to a lack of common understanding. Although cyber practitioners have developed a deeper understanding of their respective cyber activities since the recognition of cyberspace as an operational domain in 2005, this development has had a heavy focus on the generation and application of tactical-level capabilities.[11] As such, it is imperative that the operational artist has an understanding of cyberspace as an operational domain, and can apply its capabilities within an operational construct, much in the same way operational artists in the past applied airpower and mechanization into a comprehensive operational construct that dominated the battlefields of Europe in World War II.

Therefore, it is essential to develop a greater understanding of the strategic and operational implications of cyberspace as a warfighting domain. Effectively employing cyberspace power requires not only a common understanding of what constitutes cyberspace power, but also a sophisticated understanding of cyberspace as an operational domain, and its relationship to the complementary operational domains of air, land, sea, and space to establish a common point of departure for operational artists to ensure cyberspace capabilities are employed effectively across all operational domains and appropriately at all levels of war.

This paper will demonstrate the need for a comprehensive understanding of cyberspace as an operational domain to enhance the effective employment of cyberspace

---

[11] While the armed services were developing cyberspace-related capabilities (then categorized as information warfare activities) as early as 1993, cyberspace wasn't discussed in terms reminiscent of an operational domain until 2005. Derek S. Reveron, "An Introduction to National Security and Cyberspace," *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, (Washington, D.C.: Georgetown University Press, 2012), pp. 5, 9; Lalit V. Mishra, *Understanding Information Warfare: All You Need to Know*, (Alpha Edition, 2017), pp. 1-24; Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly*, Vol. 92 (1st Quarter 2019), p. 11.

power. To facilitate this, the paper will approach the discussion of cyberspace as an operational domain in three parts. Chapter One establishes a foundational understanding of cyberspace and warfare in cyberspace. Chapter Two examines the nature and character of the cyberspace domain and its strategic, operational, and tactical implications for contemporary strategists and planners. Chapter Three discusses the application of cyberspace power, focusing on its integration into the operational design process, emphasizing the importance of cyberspace as a warfighting domain through the application of cyberspace power and capabilities across all other domains at the operational level of war. The combined result provides a common point of departure for operational artists, thereby expanding their understanding of cyberspace and demonstrating the importance of leveraging deliberate processes to advance the operational design while enhancing the operational artist's appreciation of time, space, forces, and effects, as applied to the cyberspace domain.[12]

[12] The strategic guidance for cyber power is evolving. The United States Department of Defense issued two cyberspace-strategy documents in the last four years (in 2015 and 2018), and the Chairman of the Joint Chiefs of Staff codified cyber doctrine in *Cyberspace Operations*, Joint Publication 3-12 (issued in 2018). The 2018 version of *Cyberspace Operations* is an update on, and expansion of, the previous version of the document released in February 2013. Arguably of greatest benefit to the joint force is that this version of JP 3-12 was written as an unclassified document accessible to *all* Department of Defense personnel; the classified nature of the previous document greatly limited the opportunity for personnel outside cyber-focused organizations to develop understanding of cyber operations. The 2018 version of JP 3-12 is based on the 2015 Department of Defense Cyber Strategy, which has been explicitly superseded by the 2018 Department of Defense Cyber Strategy.

CHAPTER ONE: CYBERSPACE AND WAR

In order to develop the operational artist's understanding of cyberspace—and its implications in the contemporary environment—it is necessary to deliberately cultivate one's comprehension and perception of cyberspace. Development of such knowledge allows the operational artist to advance his understanding of the significant interactions between cyberspace and other elements of the operational environment; this understanding is of vital importance for planners at the operational level of war. It is important to recognize that such an understanding of cyberspace at the operational level of war does not require the operational artist to be a practitioner of cyberspace operations or even possess a technical understanding of how cyberspace operations are carried out.[1]

As Lucas Kello indicates in his book, *The Virtual Weapon and International Order*, "only the minimum degree of technical acuity is needed to reveal the scope of maneuver in the new domain."[2] Kello suggests that a set of "common technical concepts" is the baseline schema from which international relations theorists can effectively pursue development of cyberspace theory.[3] The purpose of this conceptual baseline is to "help address the rhetorical hysterics and conceptual convulsions that prevail in much of the public perception of cyber issues."[4] These issues illustrate the misunderstandings associated with cyberspace in the collective consciousness, thereby complicating discussions surrounding cyberspace and perpetuating misconceptions that

---

[1] Lucas Kello, *The Virtual Weapon and International Order*, (New Haven: Yale University Press, 2017), pp. 42-44.
[2] Ibid., p. 42.
[3] Ibid., p. 44.
[4] Ibid., p. 45.

must be countered and clarified before progress can be made.[5] As Kello states, "Cyber studies . . . part from a basis worse than zero knowledge; it [cyberspace studies] must begin from *negative* knowledge."[6] Thus, it is necessary to first develop a common understanding of the key elements of cyberspace in order to develop an understanding of cyberspace power.

This chapter moves the operational artist toward a deeper understanding of cyberspace by addressing three key elements of cyberspace: origins and contemporary manifestations of cyberspace[7], cyberspace threats, and the genesis and manifestations of cyberspace warfare.[8]

Origins and Contemporary Manifestations of Cyberspace and the Internet

The term "cyberspace" was first coined by science fiction writer William Gibson in his 1982 short story *Burning Chrome.* In 1984, Gibson defined cyberspace in his first novel, *Neuromancer,* as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation . . . a graphic representation of data abstracted from . . . every computer in the human system . . . clusters and constellations of data."[9] Gibson's description and definition of cyberspace were inspired by his observation of

---

[5] Kello, *The Virtual Weapon and International Order*, pp. 44-45.
[6] Kello's statement attempts to capture the requirement that any progress in collective understanding of cyberspace first requires the participants in the discussion to resolve the existing counterproductive notions of cyberspace (the *negative* knowledge) before productive discussions can begin. Ibid., p. 45.
[7] This element, the origins and contemporary manifestations of cyberspace, includes discussion on the origin of the internet—as manifestation of cyberspace—and the internet's effect on the operational environment.
[8] This element, the genesis and manifestations of cyberspace warfare, includes discussion on great power competition in cyberspace and its relation to warfare in the contemporary operational environment.
[9] John P. Carlin, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, ed. Garrett M. Graff, (New York, NY: Public Affairs, 2018), pp. 32-34.

young people in arcades and their fascination with the digital world (as represented by the images and stories portrayed in video games). He saw the "physical intensity of their [the kids'] posture," and recognized the effect of the digital world on these individuals.[10]

The development and proliferation of the personal computer further solidified the concept of cyberspace in Gibson's mind. He recognized that "everyone is going to want one . . . and everyone is going to want to live inside them," and that "the notional space behind all the computer screens would be one single universe."[11] The manifestation of Gibson's original concept of cyberspace remains, existing in the contemporary environment as a space where the virtual and the physical meet and reshape the other.[12]

Current joint doctrine reflects a similar understanding of cyberspace. With more technical language, *Cyberspace Operations*, Joint Publication 3-12, defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[13] The doctrinal definition is a descriptive definition that lacks Gibson's understanding of the interaction between individuals and the machine network. This is the insight from Gibson that is important for the operational artist.

The Internet

Before the internet, cyberspace existed in isolation, in the videogames and personal computers that Gibson describes, and in closed government and academic

---

[10] Carlin, *Dawn of the Code War*, p. 32.
[11] Ibid., p. 35.
[12] Ibid., p. 34.
[13] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, (Washington, D.C.: The Joint Staff, 20 November 2014), p. GL-4.

networks, barely more than a concept. The internet made cyberspace accessible to the individual, driving a technological revolution that has, and will continue to, shape the global strategic environment. Although cyberspace and the internet are inherently linked, the terms are not interchangeable. The internet is best understood as "the global network of computerized connections through which information and commerce flow."[14] Cyberspace, on the other hand, includes not only the internet, but individual computers, closed networks, and stand-alone systems around the world.

The internet got its start in 1969 with the development of ARPANET[15], a Pentagon-sponsored experiment for labs and research centers at academic institutions to transfer data and share processing power between sites as computers were being utilized and developed to support more and more labor-intensive data activities. By 1973, ARPANET had expanded from its six initial sites to 25 networked computers across the United States, and served as a network lab for early computer scientists and telecommunications engineers to develop new data transfer procedures and protocols. With the development of transmission control protocol/internet protocol, or TCP/IP, in 1983, the internet, as recognized today, was born.[16]

Concurrent with the development of the internet, theorists and strategists were starting to think about the implications of the internet and the associated rapid advance of technology. One of the earliest discussions on the subject was published in 1993 by two authors from RAND Corporation, John Arquilla and David Ronfeldt. Titled *Cyberwar Is*

---

[14] Paul J. Springer, *Cyber Warfare*, (Santa Barbara, CA: ABC-CLIO, 2015), p. 316.
[15] Advanced Research Projects Agency Network (ARPANET), the predecessor of the internet as it exists today.
[16] Carlin, *Dawn of the Code War*, p. 84.

Coming, the document examined the implications of cyberspace on national security and future warfare. Their work suggested that warfare and competition in cyberspace would manifest in two forms, "cyberwar" and "netwar", with "cyberwar" focused on military conflict and "netwar" encompassing cyberspace conflict between nations and societies below the level of war.[17] In the 27 years since their [Arquilla and Ronfeldt] work, cyberspace conflict has manifested in both "cyberwar" and "netwar", emanating from myriad cyberspace threats.

Manifestation of Cyberspace Threats

Cyberspace threats have existed since the inception of the domain. These threats evolved as cyberspace evolved. By the mid-1980s, the early manifestations of hacking had fallen prey to the increased presence of disruptive and destructive users in cyberspace, and hacking transformed from innocuous pranks to malicious activities.[18] During the last two decades of the 20th century, hacking became both a sinister and romantic term that encompassed disruptive—whether intentional or unintentional—activities in cyberspace, ranging from the Morris Worm in 1988 to the Solar Sunrise event in 1998.[19]

---

[17] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," in *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND Corporation, 1997), pp. 23-60.
[18] Carlin, *Dawn of the Code War*, pp. 77-86.
[19] The Morris Worm was the first national-level hacking event to hit the United States. The worm was a computer program that replicated itself in infected computers and attempted to gain access to additional networked computers. Within 24 hours, the program had shut down nearly ten percent of all computers connected to the internet in 1988, becoming front-page news across the country. The Solar Sunrise event was a sophisticated hacking incident where two 14-year-old kids from California, with the help of an Israeli teenager coaching them, gained mainframe-level access to the military computer networks at several Air Force bases across the United States in February, 1998. While the hackers demonstrated no malign intent, the incident highlighted the vulnerability of even protected government networks. Ibid., pp. 91-103.

Cyberspace threats continued to develop as the world moved into the 21st century. Cyberspace now offers opportunities for former and emerging great powers to reshape the geo-strategic environment while providing aspiring states, sub-state, non-state, and even individual actors an avenue to influence or improve their position in global system. Carlin describes the evolution of cyberspace threats from the late last century through the present in terms of four epochs.[20] To advance the operational artist's understanding of cyberspace threats in the contemporary environment, this paper will discuss these epochs in terms of their manifestations.[21]

The first of these manifestations arose in the late 1990s and continues today. This manifestation is characterized by the theft and exploitation of information resident in cyberspace for economic gain. This manifestation marked the beginning of China's efforts to further its global position through the theft of intellectual property to further its aspirations to become a great power. China's efforts focused on leveraging cyberspace capabilities to steal information that could be used to close the gap between its capabilities and the dominance of the United States on the global stage.[22]

---

[20] Carlin, *Dawn of the Code War*, pp. 53-57.

[21] Carlin's characterization of the four epochs described above are useful in developing a cognitive understanding of the forms that cyberspace threats may take in the operational environment. While Carlin uses the terms "epoch" and "evolution" to describe the forms cyberspace threats have taken in the 21st century, denoting distinct time periods and forms in the manifestation of these threats, the epochs and evolutionary forms he describes are not exclusionary. In fact, the use of the terms "epoch" and "evolutionary" may actually be counterproductive discussions relative to the cyberspace threats. Additionally, the term "evolution" implies a distinction between one form and the next, implying one has been replaced by another. This is not the case with cyberspace threats. For example, in the contemporary environment, what Carlin refers to as "epochs" run concurrently and may be more accurately characterized as "manifestations" of cyberspace threats than distinct periods in cyberspace threat history.

[22] Ibid., pp. 53-54,145-150.

The second manifestations emerged in the 2000s when cyberspace actors began pursuing destructive attacks in and through cyberspace, heralding what is arguably the first state use of asymmetric cyberspace warfare by Iran against the United States. [23]

The third manifestation Carlin discusses is marked by the use of social media and vulnerable communications by actors who have weaponized information to influence public opinion, undermine confidence, and foment discontent to achieve their goals. One such example is the North Korean attack on the Sony Corporation, which successfully leveraged the 24-hour news cycle and social media to spread disinformation as legitimate information and disrupt Sony's global activities.[24]

The fourth manifestation, still ongoing, is one in which actors combine operations in cyberspace with physical and destructive operations outside the cyberspace domain. Russia has demonstrated this type of activity in Georgia in 2008 and Ukraine in 2014.[25] This capability does not solely belong to the nation-state. Non-state actors have used similar tactics. The Islamic State of Iraq and the Levant (ISIL) has been active in this manifestation as well, leveraging cyberspace recruitment to facilitate operations in areas outside of ISIL control.[26] This tactic of blending cyberspace operations with destructive or disruptive operations through or outside the cyberspace domain threatens all aspects of society, from the availability of emergency and critical services to trust in financial and government institutions.[27]

---

[23] "The attack by Iranian actors on the Sands Casino was arguably the first destructive nation-state cyberattack inside the United States." Ibid., pp. 54.
[24] Carlin, *Dawn of the Code War*, pp. 54-56.
[25] Dennis F. Poindexter, *The New Cyberwar: Technology and the Redefinition of Warfare*, (Jefferson, NC: McFarland, 2015), pp. 14-18.
[26] Carlin, *Dawn of the Code War*, pp. 1-29.
[27] Ibid., pp. 56-57.

The fifth manifestation is also ongoing, and represents one of the most important operational aspects of contemporary cyberspace—the threat of the rogue actor. The rogue actor conducts operations in cyberspace for personal gain; whether that personal gain comes in the form of ideological satisfaction of monetary gain, the motivations ultimately fall below the level of statecraft. As such, these actors, operating independently or as proxies of a state, closely resemble privateers and pirates of great naval epochs past, operating below the level of the state as sub-systemic manifestations.[28]

While the five manifestations of cyberspace threats outlined here (economic espionage, destructive attacks, attacking what is known, synchronized cross-domain attacks, and rogue actors) give the operational artist an understanding of how those threats may present themselves in the contemporary operational environment, two common themes or purposes can be seen in their respective activities. The two common themes of threat actors operating in the cyberspace domain can be further characterized by their effects: the first effect, denying an opponent the opportunity to leverage their capabilities or advantage; the second effect, manipulating information to generate socio-psychological effects on a target audience.

The first of these effects, denial, is an effect that is well known, as it is consistent with historical and contemporary military doctrine.[29] In terms of hostile cyberspace activity, denial encompasses an adversary's efforts to deny friendly force freedom of

---

[28] Florian Egloff, "Cybersecurity and the Age of Privateering," in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel E. Levite, (Washington, D.C.: Georgetown University Press, 2017), pp. 231-244; Kello, *The Virtual Weapon and International Order*, pp. 254-255.

[29] Denial is included in *Joint Fires*, Joint Publication 3-09, as one of several effects generated by fires. These effects include "destroy, delay, deny, neutralize, suppress, or influence." Office of the Chairman of the Joint Chiefs of Staff, *Joint Fires*, Joint Publication 3-09, (Washington, D.C.: The Joint Staff, 10 April 2019), p. I-2.

maneuver (FoM) and freedom of action (FoA), or deny friendly force relative advantage in capability (military, economic, technological, etc.). This is consistent with the concept of "cyberwar" described by John Arquilla and David Ronfeldt 27 years ago. Operationally, denial can be accomplished by disrupting command and control mechanisms, thereby delaying the flow of information, and ultimately denying the affected actor the ability to maneuver its forces in space and time to counter adversary action, as Russia has attempted multiple times over the last two decades.

The second effect, manipulation, is the lesser understood of the two. While manipulating information in cyberspace can support denial effects, such as changing information to confuse and delay action by an actor, it also has the ability to attack and alter the perceptions of societies themselves. Manipulation of military or government information can complicate an actor's response to aggressive behavior, potentially giving an adversary a marked advantage, should the conflict escalate into violence. The operational artist should not overlook this aspect of manipulation; the power of cyberspace operations to shape what is known by a target audience influences the psycho-social dimension of societies, and, ultimately, the individual members of the target society. The ability of cyberspace activities to change or reinforce attitudes and perceptions, and to establish and maintain conditions and narratives favorable to operational and strategic objectives, cannot be underestimated.[30] The ability to attack a society at the state or individual level is a new and largely untested operational-strategic aspect of this new warfighting domain.

---

[30] This psycho-social element of cyberspace threat activities is reminiscent of Arquilla and Ronfeldt's description of "netwar", which they characterized as efforts to disrupt a society's view of itself and the world around it. Arquilla and Ronfeldt, "Cyberwar Is Coming!", pp. 28-30.

Genesis of Cyberspace Warfare

Understanding and differentiating between cyberspace threats and cyberspace warfare hinges on the understanding of war and warfare itself.

In the classical, or Clausewitzian sense, war is characterized as "an instrument of politics," and "an act of force to compel our enemy to do our will." [31] Clausewitz also contended that, once initiated, war tends toward extremes in the "use of force . . . disarmament of the enemy . . . [and] exertion of strength."[32] In this manifestation, war is the domain of the state; war is concentrated force, tending towards extremes, wielded by the state as a "continuation of policy,"[33] in pursuit of clear objectives, inseparable from the relationship between the people, the military, and the state.[34] The classical understanding of war, also called "old wars", results from an environment dominated by sovereign states and large-scale, state-centered, and state-supported wars. This definition dominated war theory through the 20th century and still shapes the Western understanding of war.[35]

Contemporary manifestations of war encompass wars from the late 20th century through the present day, and are characterized by contemporary war theorists as "new wars".[36] These wars coincided with the phenomenon of globalization, and reflect the conditions of the environment that resulted from globalization, a major feature of which

---

[31] Herfried Munkler, *The New Wars*, (Cambridge, UK: Polity Press, 2005), p. 13.
[32] Carl Von Clausewitz, *On War*, (New York: Everyman's Library, 1993), pp. 83, 85-86, 737.
[33] Ibid., p. 99.
[34] Ibid., pp. 83-101.
[35] Kaldor, *New and Old Wars: Organized Violence in a Global Era*, 3rd Edition, (Stanford: Polity Press, 2012), pp. 15-17.
[36] Munkler, *The New Wars*, p.13; Kaldor, *New and Old Wars: Organized Violence in a Global Era*, 3rd Edition, pp. 15-31.

is the erosion of the state's monopoly on war.[37] Mary Kaldor incorporates this condition in her definition of war as "an act of violence involving two or more organised groups framed in political terms."[38] New war, then, is distributed force, tending towards expansion of violence in space and time, wielded in pursuit of ambiguous and often changing objectives.[39] In these new wars, the political actor has supplanted the Clausewitzian state.

The complexity of the current, and likely future, geopolitical and geostrategic environments is exacerbated by the duality of old and new wars in the operational environment today. For the terms "war" and "warfare" to remain useful in today's discussions—especially in conceptualizing cyberspace warfare—war must be redefined in the context of the global environment. In contemporary terms, influencing what is known, rather than solely using violence to compel, is the decisive element in modern war and warfare. To that end, war can be defined as the application of violence by an organized group to influence the environment in pursuit of political objectives, legitimized by the group's constituency, and at all times influenced by their respective perception of their environment. This definition of war accommodates new war and cyberspace war concepts, and provides the necessary foundation from which a contemporary definition of warfare can be derived.

---

[37] Kaldor, *New and Old Wars: Organized Violence in a Global Era*, 3rd Edition, pp. 71-93.
[38] Mary Kaldor, "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?", *Global Policy*, 3, Issue 10, (October 2010), p. 274.
[39] Munkler, *The New Wars*, pp. 8-13.

The term "warfare" appears 139 times in the *Department of Defense Dictionary of Military and Associated Terms*; yet, warfare itself remains undefined in joint doctrine.[40] Therefore, warfare is defined as encompassing all aspects of military, or para-military, operations normally conducted during wars or conflict among states, sub-states, and non-state actors, to advance an actor's interests while degrading, denying, destroying, influencing, or neutralizing an adversary's ability to do the same. In the context of cyberspace warfare, to be successful, the operational artist must be able to understand war as it is influenced by cyberspace and to differentiate between disruptive and destructive cyberspace activities. Applied to cyberspace, cyberspace warfare can be defined as all aspects of military, or para-military, operations in cyberspace normally conducted during wars or conflict among states, sub-states, and non-state actors, to advance an actor's interests while degrading, denying, destroying, influencing, or neutralizing an adversary's ability to do the same.

This definition of war and warfare adapted to a new warfighting domain is borne out by three examples from recent history.

Months and even years prior to Russia's military invasion and annexation of the sovereign Ukrainian territory of Crimea in February and March of 2014, Russia was executing information warfare to influence its neighbor as a buffer against Western

---

[40] In the 206 pages of definitions listed in the *Department of Defense Dictionary of Military and Associated Terms*, January 2020, the term "cyberspace warfare" is absent. The term "cyberspace" appears 37 times in those 206 pages, with one of those instances defining cyberspace and 12 more including cyberspace as a portion of the term being defined (cyberspace attack, cyberspace capability, cyberspace defense, cyberspace operations, etc.). The term "warfare" appears 116 times in those same 206 pages, with warfare being included as a portion of the term being defined 23 times (antisubmarine warfare, chemical warfare, electronic warfare, irregular warfare, etc.); yet, the term "warfare" itself is undefined. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, (Washington, D.C.: The Joint Staff, January 2020), pp. 6-237.

influence.[41] With the advent of the cyberspace domain, Russia found a new mechanism through which it could manipulate the psycho-social environment to achieve its ends. In 2013, Russia developed a new doctrine to take advantage of the information opportunities inherent in the openness of the cyberspace domain, leveraging social media in conjunction with proxy groups to undermine anti-Russian groups and foster fear, resentment, and anti-Ukrainian government sentiment among ethnic Russians while stirring Russian patriotism within the Ukraine's ethnic Russian population.[42] As Kello suggests, Russia's use of cyberspace "is not to augment war . . . but to circumvent it by opposing the adversary where his vulnerability is greatest . . . in the disruption of the open and sometimes fragile information spaces of liberal democracies."[43]

In the four months between the catalyzing event of the crisis in Ukraine and the annexation of Crimea, Russia was able to wage a robust information warfare campaign in and through the cyberspace domain while preparing forces for a rapid takeover of political and military nodes.[44] Russian actors conducted additional cyberspace operations

---

[41] Elizabeth A. Wood, William E. Pomeranz, E. Wayne Merry, and Maxim Trudolyubov, *Roots of Russia's War in Ukraine*, (New York: Columbia University Press, 2016), pp. xii-xiii, 14-16; Bobo Lo, *Russia and the New World Disorder*, (Washington D.C.: Brookings Institute Press, 2016), pp. 100-112. (http://www.jstor.org/stable/10.7864/j.ctt6wpccc.9).

[42] The Gerasimov Doctrine is incorrectly named for Russian General Valery Vasilevich Gerasimov, Russian Federation Chief of the General Staff. This approach to information warfare focuses on exploiting the seams between Russian and Western spheres of influence, where weak liberal democracies can be exploited. Kello, *The Virtual Weapon and International Order*, pp. 216-221; Wood, *Roots of Russia's War in Ukraine*, pp. xi-xiv, 12-16.

[43] Full quote: "The doctrine's main purpose is not to augment war, though this may be so in limited instances, but to *circumvent* it by opposing the adversary where his vulnerability is greatest and his doctrinal understanding retarded: in the disruption of the open and sometimes fragile information spaces of liberal democracies." Kello, *The Virtual Weapon and International Order*, p. 219.

[44] The Maidan protests took place in Kiev, Ukraine, following the refusal of Ukrainian president Viktor Yanukovych to sign an Association Agreement with the European Union (EU). Yanukovych's heavy-handed response resulted in nearly 100 deaths and led to additional protests and calls for Yanukovych's removal. Wood, *Roots of Russia's War in Ukraine*, pp. xi-xiv.

to disrupt Ukrainian command and control as well as communication networks.[45] Russian preparation of the battlespace and coordination of cross-domain air, land, sea, and space operations enabled Russia to occupy sovereign Ukrainian territory with practically no resistance. Since that time, Russia has continued to leverage the cyberspace domain to further its objectives, leveraging "troll armies" to counter anti-Russian sentiment and paint Russian actions in positive and patriotic tones.[46] Now, more than six years later, the world has largely acquiesced to Russia's declaration of sovereignty over Crimea.

Iran's cyberspace attack on the Sands Casino in Las Vegas, Nevada, in 2014, is considered the first destructive cyberspace attack by a nation state against a target in the United States homeland.[47] Three months prior to the attacks, in October 2013, Sheldon Adelson, the owner of the Sands Casino and an outspoken supporter of Israel, made a statement suggesting that the United States needed to take a harder line with Iran. In November 2013, Ayatollah Khamenei, the Supreme Leader of Iran, responded saying, "these prattling people . . . should receive a slap in the mouth."[48] In January 2014, Iranian hackers began a series of cyberspace attacks on Adelson's resort and casino enterprise. By February 10, 2014, the Iranian hackers had infiltrated nearly every computer across the company, shutting down servers, erasing hard drives, and corrupting files to the point they were unrecoverable. The hackers also stole personally identifiable information for tens of thousands of customers and employees. Estimates of the physical

[45] Poindexter, *The New Cyberwar*, pp. 34-36.
[46] Kello, *The Virtual Weapon and International Order,* pp. 219-220.
[47] Carlin, *Dawn of the Code War*, pp. 54, 234.
[48] Ibid., pp. 234-235.

damage to the company's infrastructure totaled nearly $40 million.[49] The attackers made their motivations clear—retribution for Adelson's comments regarding United States policy toward Iran.[50] The attack did not target critical infrastructure, the national government, or the national security apparatus; it illustrated what an actor—or actors working in concert toward a single objective—could do to vulnerable systems.

The horrors perpetuated by violent extremist organizations, such as al-Qaeda and the Islamic State of Iraq and the Levant (ISIL), have been spread across the internet for the world to see. Many of these digital activities focused on terrorism finance and waging information warfare through propaganda and misinformation to build support for their respective causes. These groups have also sought to use cyberspace to recruit, encourage, and facilitate violent attacks against targets beyond their physical control. Junaid Hussain was one of several ISIL recruiters for the CyberCaliphate. In 2015, his recruiting efforts had been so successful that the Federal Bureau of Investigation (FBI) was having difficulty keeping up with ISIL recruits spread across the United States; at least nine of Hussain's recruits were reportedly captured or killed by law enforcement as they attempted to execute their terror campaign on United States soil. Hussain also leveraged cyberspace capabilities to obtain names and addresses of 1,351 United States military personnel as well as a "kill list" of 100 United States Air Force personnel.[51]

Great Power Competition in Cyberspace

Cyberspace has altered more than just warfare; it has affected the manner in which actors, and, more specifically, great powers, interact in the geostrategic

[49] Carlin, *Dawn of the Code War*, pp. 234-239.
[50] Ibid., p. 238.
[51] Ibid., pp. 19-23.

environment. States and non-states recognize the power of cyberspace as an operational domain to influence people, shape what is known, and support complementary political, diplomatic, economic, or military actions. We are already seeing how warfare has been altered by Russia and Iran, as well as by sophisticated non-state actors. China's use of cyberspace capabilities to bolster its position in the geo-strategic environment offers an excellent example of the use of cyberspace warfare at the strategic level—an example of great-power competition.[52]

China's cyberspace activity has largely focused on advancing its regional and global position in terms of economic power and military capability. China viewed the cyberspace domain and, specifically, the openness of the internet, as a tool to "hasten its rise, growth, and modernization."[53] Development of the domestic and export economy was a major focus of Chinese cyberspace activities. China, with its state-owned economic model, engaged in government-sponsored economic espionage to steal technology, bypassing costly research and development activities and moving to direct competition with those they had stolen from.[54] While the United States views China's theft of intellectual property for economic benefit as a crime, China simply views their actions as a natural extension warfare.

---

[52] As with the term "warfare" in the previous section, there is no definition for "great power competition" in the *Department of Defense Dictionary of Military and Associated Terms*. Again, the operational artist must determine for himself what great power competition is and is not. As such, the following definition of great power competition is offered: great power competition is the series of interactions between internationally recognized political entities possessing a combination of global economic, global military, or global political influence or capability to either gain or maintain geo-strategic advantage while denying, degrading, or neutralizing a competitor's ability to do the same.

[53] Carlin, *Dawn of the Code War*, p. 147.

[54] Ibid., pp. 142-150.

China's effort to compete in and through the cyberspace domain is not limited to cyberspace crime; Chinese leaders have declared the internet a battlefield and developed cyberspace strategies to leverage its citizens, not just its military, to conduct cyberspace operations. The Chinese have created a hybrid model of state and rogue actors working in concert for a specific objective.[55] Although China's activities in cyberspace do not reach the threshold of war, China continues its strategic and operational warfare campaigns, leveraging, to its benefit, the space that exists between peace and war.

Warfare in Cyberspace: A Summary

This discussion of cyberspace focuses on three elements key to the operational artist's understanding of cyberspace as it relates to the influence cyberspace has on the geo-strategic environment, the interaction between actors in that environment, and the mechanisms through which those interactions take place.

The first element highlights the conceptualization of cyberspace from socio-cultural and scientific aspects, as well as the implications of the internet-fueled expansion of cyberspace beyond the realm of the state.

The second element focuses on the fundamental aspects of cyberspace threats. Conceptualizing cyberspace threats aids the operational artist in developing a cognitive understanding of the character of threats in cyberspace by separating cyberspace threats based on actor and intended effects; doing so is essential to a better understanding of the cyberspace domain in terms of its effect on the operational environment and its integration with other military activities to facilitate cross-domain operations in support of United States strategic interests.

---

[55] Carlin, *Dawn of the Code War*, pp. 148-149.

The third element examines the contests between state, sub-state, and non-state actors and the respective manifestations of those contests in cyberspace. The encroachment of cyberspace into nearly every aspect of daily life has fundamentally altered the geopolitical, socio-cultural, and geostrategic environments, as well as the interaction of all actors engaging in the global environment. Cyberspace has altered the traditional understanding of war and warfare itself. The examples of cyberspace warfare—and its manifestation in conflicts between states, sub-state, non-state, and individual actors—further demonstrate how cyberspace has been, and will continue to be, leveraged in war and in the space that exists between peace and war.

Cyberspace, unlike air, land, sea, and space, has undermined the sovereignty of the state over war and warfare. Cyberspace has also laid societies bare in a manner unprecedented in human history, a fact that adversaries of the United States have not overlooked. Threat actors of all types can leverage this vulnerability to gain an asymmetric advantage over a given state, socio-cultural group, organization, or even an individual. The psycho-social dimension of societies has become the primary target, and its manipulation is intended to shape what is known within the target audience, unconstrained by geography, or even time. For states, cyberspace warfare has economic and political influence capabilities; for non-states, it has proxy support. The cyberspace domain is increasingly where states and non-states seek strategic and operational advantage.

These three foundational elements provide a common point of departure for the operational artist to build an understanding of cyberspace as it relates to the strategic and operational levels of war and, ultimately, an understanding of cyberspace warfare itself.

Those who fail to incorporate cyberspace power at the operational level of war, and to develop a common understanding of cyberspace as an operational domain, risk their place and relevance in the geostrategic environment.

CHAPTER TWO:

CYBERSPACE IMPLICATIONS FOR THE OPERATIONAL ARTIST

This chapter advances the operational artist's understanding of cyberspace by addressing three key elements of cyberspace as an operational domain: the *conceptualization* of cyberspace as an operational domain, the *nature* of cyberspace as an operational domain, and the *implications* of cyberspace as an operational domain.

Cyberspace as an Operational Domain[1]

There is a duality to cyberspace; one aspect is rooted in the traditional concept of states, while an opposing aspect is cultivated through globalization. Taken as a whole, cyberspace has changed the way individuals, socio-cultural groups, and states view the world and their place in it, thereby generating dramatic effects on the operational environment. Current joint doctrine views cyberspace activities in terms of the effects they have on the operational environment; with the establishment of information as an independent joint function, the doctrinal definition of the information environment is "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information," this is an attempt to combine all elements of information and cyberspace, and is the premise under which the Department of Defense currently views all information-related capabilities. [2]

---

[1] For a detailed survey of current joint doctrinal definitions, see the following publications: Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, (Washington, D.C.: The Joint Staff, 8 June 2018), pp. GL-4, I-7, II-5; Office of the Chairman of the Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, (Washington, D.C.: The Joint Staff, 17 January 2017), p. iii; Office of the Chairman of the Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, D.C.: The Joint Staff, 20 November 2014), p. ix.

[2] Office of the Chairman of the Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, D.C.: The Joint Staff, 20 November 2014), p. ix; Office of the Chairman of the Joint Chiefs of Staff, *Joint Operations*, pp. III-17-III-27.

United States *Cyberspace Operations* doctrine (Joint Publication 3-12) describes the basic elements of the cyberspace domain as distinct layers of a larger system, each representing an aspect of the domain: the physical network layer, the logical network layer, and the cyber-persona layer.

The physical network layer of the domain includes all of the physical components of networks (e.g., routers, switches, computers, data storage centers, smart phones), their geographic location, and the communications links between the networks, whether they are closed or open, co-located or geographically separate.[3]

The logical network layer of cyberspace encompasses all the information and logic processes (code) resident, either permanently or temporarily, in computer and data management systems. The logical network layer of cyberspace complicates locating and targeting cyberspace actors, as it is the mechanism by which they can mask their locations and carry on threat activities distinct from their physical location. Consequently, targeting through traditional warfighting domains, which, only acting in the physical space, relies on the physical capture or destruction of the threat, becomes increasingly difficult. Therefore, cyberspace activities are the only mechanisms through which the United States can target threats within the logical network layer of cyberspace.[4]

The cyber-persona layer represents the socio-psychological element of the cyberspace domain; it is the layer at which individuals, either on their own behalf or on that of another individual or entity, interact with, and within, the domain. This layer encompasses all aspects of an individual or entity's cyberspace activities and associated

---

[3] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, pp. I-3, IV-9.
[4] Ibid., pp. I-4, IV-9.

accounts, and identifiable information as well as their interaction and linkages with other actors active within the domain. The information collected and grouped relative to a particular entity is called a cyber-persona. Doctrinally, the cyber-persona layer is used to facilitate greater understanding of actors in the operational environment, linking them to portions of the physical and logical network layers of cyberspace that can be targeted and engaged by the joint force.[5] Through information operations, and other information-related capabilities, the operational artist can influence the socio-psychological aspects of target audiences. The access to target audiences that the cyberspace domain provides is unprecedented and represents a mechanism through which the operational environment can be shaped to facilitate the realization of desired ends.

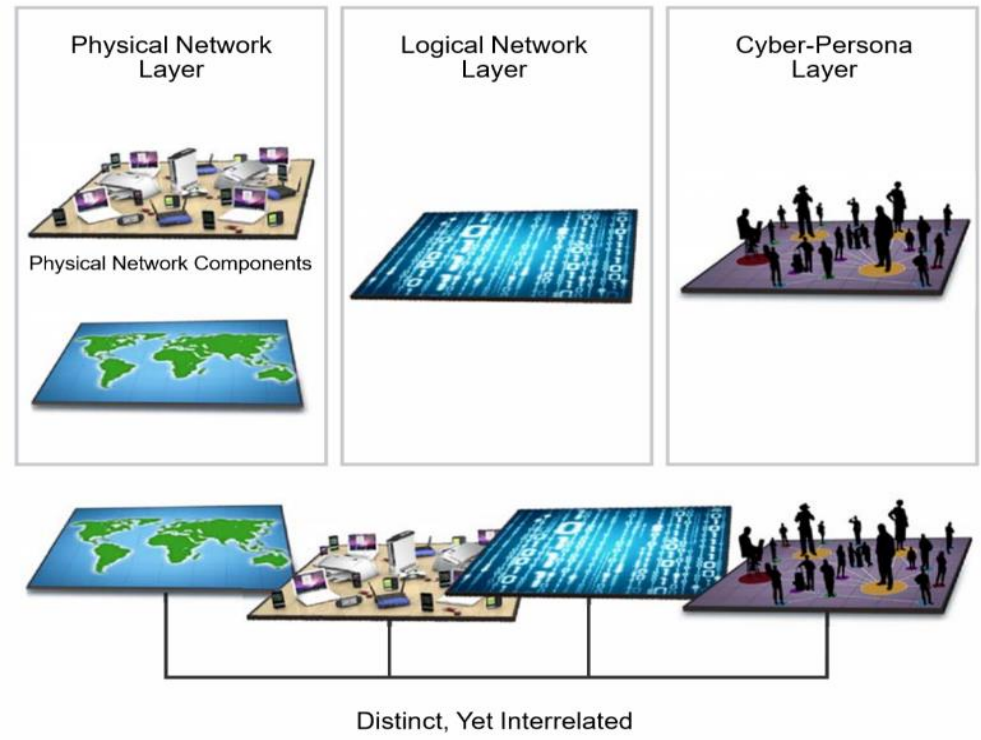


Figure 1: The Three Interrelated Layers of Cyberspace[6]

[5] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, pp. I-4, IV-9.
[6] Ibid., p. I-3.

The Nature of Cyberspace

The conceptualization of cyberspace as an operational domain contributes to the understanding of the nature of a warfighting domain. The cyberspace domain is unlike other operational domains, in that cyberspace is not a natural domain. In the instance of the air, land, sea, and space domains, man observed the domains and developed mechanisms to use them to his benefit. In the case of the cyberspace domain, man observed the limitations of the other four domains and developed a mechanism to transcend those limitations.

As cyberspace expanded, it transcended state boundaries and the physical barriers of geography and space, linking individuals and societies in ways that could only be imagined in the last century; however, this aspect of the cyberspace domain comes into conflict with the reality that the physical components of the information systems necessary for the existence of the domain reside within the traditional construct of the nation-state system. In other words, as related to information and human interaction, the cyberspace domain has transcended geography, space, and the nation-state system, but no portion of cyberspace exists outside the sovereign reach of the state.

Implications for Operations in the Cyberspace Domain

As its nature reflects, cyberspace has significant implications for contemporary and future operational environments. Cyberspace presents implications for global operations that leverage the cyberspace domain to achieve objectives within the operational environment. These include: the Department of Defense's operational space within the domain, the Department of Defense's operational activities in the domain, and

the operational artist's understanding of Department of Defense operations in and through the domain.

The operational artist's understanding of the operational space within the cyberspace domain has significant implications for the planning and execution of cyberspace activities. Unlike the other domains where the state can establish primacy, in cyberspace, the state must rely on private entities to provide for their own security and defense.[7] All operational space within the cyberspace domain is owned by an actor, whether that actor is an individual, a corporation, or a state. This condition requires that activities in cyberspace be viewed in the context of the unique conditions that exist in the cyberspace domain.[8]

United States cyberspace doctrine captures the complexity of the operational space within the cyberspace domain, dividing that space into three categories: Department-of-Defense-protected segments of cyberspace, called blue cyberspace; adversary-protected segments of cyberspace, called red cyberspace; and segments of cyberspace not protected or controlled by the United States or an adversary, called gray cyberspace.[9]

Blue cyberspace encompasses all Department-of-Defense-protected segments of cyberspace. United States activities in blue cyberspace are focused on security and defense of critical information networks and infrastructure, specifically: cyberspace security, cyberspace defense, and development of countermeasures. Cyberspace defense activities in blue cyberspace focus on identifying and defeating specific threats to DoD-

---

[7] Carlin, *Dawn of the Code War*, pp. 56-61.
[8] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, p. I-3-5.
[9] Ibid., p. I-12.

protected cyberspace. Development of cyberspace countermeasures in blue cyberspace can be offensive or defensive in nature, and focus on defeating or preventing adversary actions in—or efforts to access, exploit, or attack—protected cyberspace.

The concept of red cyberspace mirrors that of blue cyberspace, in that it is the portion of cyberspace protected and utilized exclusively by an adversary to support day-to-day operations across the operational domains. Gray cyberspace, however, is populated by both friendly and adversary elements, public and private entities, states and individuals, with the hardware that supports this segment ultimately residing within the sovereign borders of a multitude of states. As such, red and gray cyberspace, while distinct from one another, encompass the portions of cyberspace outside the Department of Defense's purview and are therefore viewed similarly, especially in terms of the cyberspace activities the department conducts in these segments of cyberspace.[10] Figure 2 depicts the complex relationships of blue, gray, and red cyberspace as related to Department of Defense activities in cyberspace.

[10] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, pp. I-2-I-7.

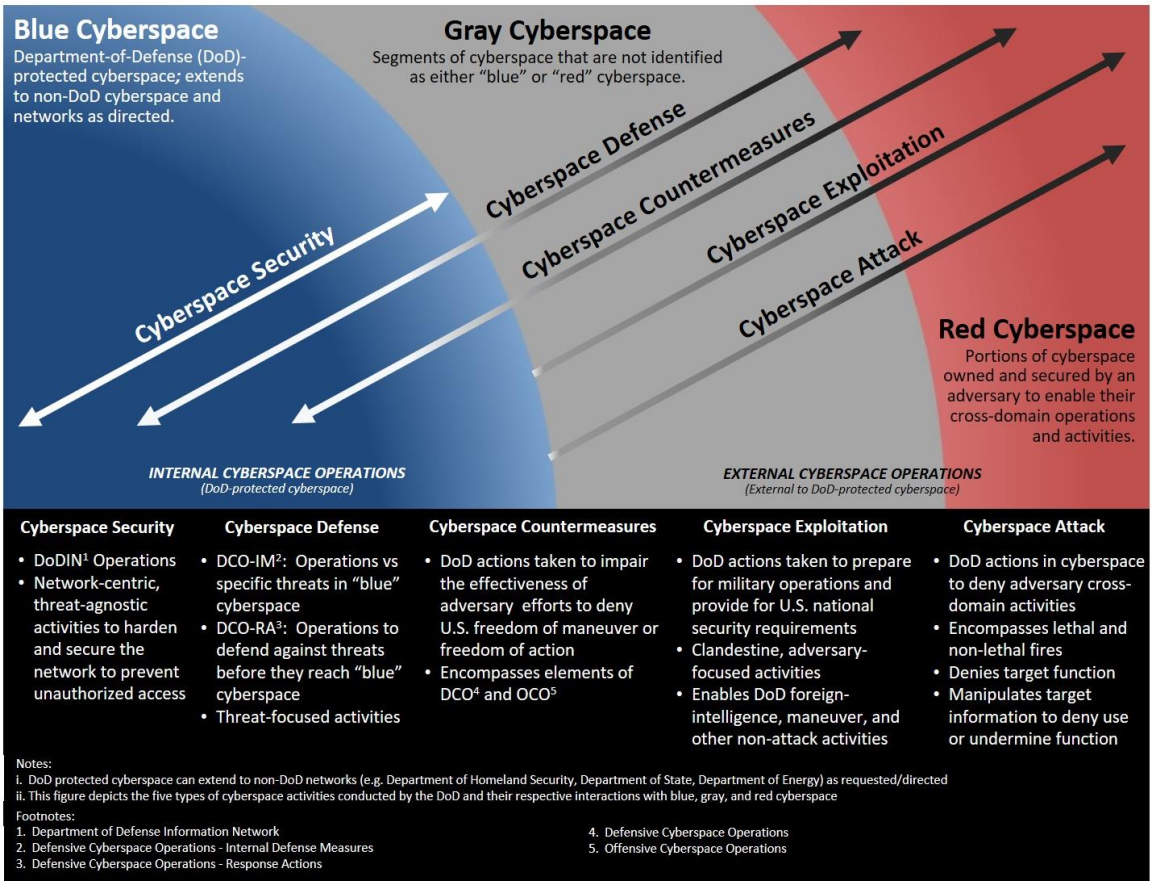


Figure 2: United States Department of Defense Cyberspace Activities[11]

Department of Defense cyberspace activities in red and gray cyberspace fall within four categories: cyberspace defense, cyberspace countermeasures, cyberspace exploitation, and cyberspace attack. While cyberspace defense and cyberspace countermeasure activities in red and gray cyberspace serve a similar purpose to those activities taken in blue cyberspace, the focus of the activities is different. Cyberspace defense in red and gray cyberspace focuses on identifying and defeating specific threats

[11] This figure was generated by the author and depicts the five types of cyberspace activities conducted by the Department of Defense, and their respective interactions with blue, gray, and red cyberspace. (The representation was derived from Joint Publication 3-12, *Cyberspace Operations*, and was modeled after a similar depiction of cyberspace as presented in the Marine Corps Cyberspace Warfare Group Command Brief, accessed 17 February 2020).

to department- and partner-protected cyberspace prior to the threat penetrating one of these networks. Development of cyberspace countermeasures in red and gray cyberspace is focused on denying an adversary the ability to leverage cyberspace against friendly forces.

Cyberspace exploitation activities are enabling functions and serve to support current operations, prepare the Department of Defense for future operations, and support national security objectives. Cyberspace exploitation includes intelligence activities as well as activities undertaken by the department to gain a positional or informational advantage in the cyberspace domain itself. Exploitation activities are not attack mechanisms, relying on their clandestine nature to be effective. Current cyberspace doctrine describes cyberspace exploitation as an offensive activity, falling under the construct of offensive cyberspace operations.[12]

---

[12] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations,* p. II-6; This perspective is supported by some cyberspace theorists who argue that cyberspace exploitation is active manipulation of the cyberspace environment and exceeds what they view as the traditional passive monitoring of an adversary. In some respects, this may be true. For example, in the air domain, a theater-level reconnaissance platform actively maneuvering and operating in the air space above or near a combat zone could be considered an offensive operation; the same could be true for an intelligence collection activity in cyberspace, provided it takes place under similar circumstances to those described in the air domain example. However, if the intelligence collection activity in cyberspace is divorced from combat, it would fall under the umbrella of espionage and statecraft rather than offensive operations. As David Fuller suggests, the cyberspace domain has created conditions that support "high-intensity espionage," not offensive activities. Joint doctrine's characterization of intelligence activities in cyberspace as offensive is inconsistent with the very same doctrine's statement that all department activities in cyberspace are characterized "exclusively by the types of effects they create." The above demonstrates the dissonance that exists within current cyberspace doctrine and demonstrates why the operational artist must develop a deeper understanding of cyberspace at the operational level. Kello, *The Virtual Weapon and International Order*, pp. 53-55; David P. Fidler, "Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, (Georgetown University Press, Washington, D.C. 2012), pp. 74-75; Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, p. II-5.

Cyberspace attack activities—also recognized as a form of fires—deny, degrade, disrupt, destroy, or neutralize an adversary's ability to perform an activity or function. The Department of Defense conducts, under specific authorities, cyberspace attack activities in red and gray cyberspace to provide a marked advantage over an adversary in pursuit of operational objectives and desired end states.[13] The traditional understanding of attack, and fires, is generally focused on adversary forces and/or capabilities. While many of the mechanisms through which cyberspace attack activities can be executed have the potential to affect traditional targets, the nature of the cyberspace domain and its pervasiveness in the contemporary environment provide new mechanisms for engagement of target capabilities, functions, forces, and audiences.

For the operational artist, understanding the effects that can be achieved by leveraging these new operational vectors is absolutely vital to building a common understanding of cyberspace operations and how cyberspace activities can be ordered in time and space, by friendly and adversary actors, to support achievement of objectives at the operational level of war. The five elements, or focus areas of cyberspace activities, discussed above, and illustrated in Figure 2, capture the operational aspects of functioning withing blue, gray, and red cyberspace. The matrix depicted in Figure 3 links the Department of Defense cyberspace activities with the cyberspace mission forces that execute those activities, and is a tool for the operational artist to use when applying cyberspace activities within the imaginative construct of the operational art. Armed with this deeper conceptual understanding of cyberspace, the operational artist can begin to

[13] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, p. II-7.

develop practical understanding of the operational employment of cyberspace activities within the doctrinal concepts of employing air, land, sea, space, and cyberspace forces.

		Cyberspace Mission Forces					
Cyberspace Activities		Cyberspace Protection Team (CPT)	Combat Mission Team (CMT)	Combat Support Team (CST)	National Mission Team (NMT)	National Support Team (NST)	Mission-Tailored Force Package (MTFP)
Cyberspace Security	DoDIN						
	Other						
Cyberspace Defense	Internal Cyberspace						
	External Cyberspace						
Cyberspace Countermeasures	OCO						
	DCO						
Cyberspace Exploitation	Intelligence						
	Maneuver						
Cyberspace Attack	Nonlethal Fires (Manipulate)						
	Lethal Fires (Destroy)						

Figure 3: United States Cyberspace Mission Forces and Activities[14]

The effects of Department of Defense operations that leverage cyberspace, and of cyberspace operations themselves—to included Department of Defense Information Network (DoDIN) activities that support Department of Defense information and communications networks—can manifest in cyberspace itself, in the other domains or environments outside cyberspace, or both. The depiction of cyberspace as an operational domain (from Figure 2) assists the operational artist in recognizing these distinctions and, coupled with Figure 3 and Figure 4, allows the operational artist to conceptualize cyberspace operations in a manner that facilitates their coordination with, and

[14] This figure was created by the author and depicts the five types of cyberspace activities conducted by the Department of Defense and the associated cyberspace mission force (CMF).

incorporation into, lines of operation, both as independent and complementary activities supporting cross-domain operations.

In addition to Department of Defense operations that generate effects *in* or *through* cyberspace, some cyberspace activities generate effects *in* and *through* cyberspace. For example, an operational planning team has identified the defeat of an adversary's integrated air defense system (IADS) as a decisive point in a line of operations. As such, a cyberspace attack is executed—in this case, non-lethal fires—targeting the integrity and availability of the information resident within the system in order to deny the adversary the functionality of their IADS. As a result, the functionality of the system is denied to the adversary, providing the attacking force a marked advantage over their adversary. In this scenario, the cyberspace activity targeted elements of red cyberspace that generated effects *in* cyberspace, the logical network layer discussed above, while simultaneously generating effects in other domains, *through* cyberspace, denied functionality of the IADS to engage in operations in physical space.

Joint Force Elements	Cyberspace Activities									
	Cyberspace Security		Cyberspace Defense		Cyberspace Countermeasures		Cyberspace Exploitation		Cyberspace Attack	
	DoDIN	Other	Internal Cyberspace	External Cyberspace	OCO	DCO	Intelligence	Maneuver	Nonlethal Fires (Manipulate)	Lethal Fires (Destroy)
Air Component										
Land Component										
Maritime Component										
Space Component										
Special Operations Component										
Inter-Agency										
Other										

Figure 4: United States Cyberspace Activities and The Joint Force[15]

Cyberspace operations *in* the cyberspace domain are actions taken in cyberspace that generate effects in cyberspace. For example, a team responsible for defending blue cyberspace identifies a specific cyberspace threat actor attempting to penetrate a protected network. The team takes action in cyberspace to isolate and destroy the threat, thereby protecting the integrity of the network and the availability of the information retained therein. The action undertaken, and the effect generated, were wholly contained within the cyberspace domain.

In addition to recognizing cyberspace operations that generate effects in the domain, the operational artist must also recognize that operations in the cyberspace domain favor the offense. Offensive operations in cyberspace create conditions in the operational environment far faster than the network-centric nature of cyberspace security can respond. This reality makes understanding and prioritizing the importance of cyberspace activities in cyberspace of critical importance to the operational artist, both in

[15] This figure was created by the author and provides the operational artist a mechanism by which the artist can organize cyberspace activities as they relate to joint force components.

ensuring the integrity of blue cyberspace and in targeting adversaries in gray and red cyberspace.[16]

Department-of-Defense activities that leverage the cyberspace domain to generate effects outside cyberspace can be characterized as operations *through* cyberspace. Operations through cyberspace encompass a range of activities from the use of digital maintenance logs and software programs that facilitate the operational readiness of Department of Defense aviation or maritime assets, to the command and control networks that facilitate the operations of remotely-piloted aircraft conducting combat operations half-way around the globe. In each of these examples, Department-of-Defense activities leverage cyberspace to generate effects outside the cyberspace domain; however, the ability of the department to conduct these activities is dependent on the availability, integrity, and security of blue cyberspace, all of which are enabled by cyberspace activities undertaken *in* cyberspace.[17]

Developing an understanding of the distinctions between effects *in* and/or *through* cyberspace is necessary to cultivating a greater understanding of the application of cyberspace capabilities at the operational level of war. The examples presented in this section, combined with the conceptualization of cyberspace (Figure 2) and design tools (Figures 3 and 4) introduced here, serve to illustrate the transition of understanding of cyberspace as an operational domain from concept to operational art. Not only does this understanding aid the operational artist in determining when and where cyberspace

---

[16] David Aucsmith, *A Theory of War in the Cyber Domain: Part 1, An Historical Perspective*, (USA: Microsoft Institute for Advanced Technology in Governments, 5 March 2012), pp. 1-17, 25-26.
[17] Aucsmith, *A Theory of War in the Cyber Domain*, pp. 1-9.

activities can be applied to generate the desired effects in gray and red cyberspace, this understanding allows the operational artist to identify the joint force capabilities that must be protected in blue cyberspace to generate the desired effects in cyberspace and the air, land, sea, and space domains.

Cyberspace and the Operational Artist: A Summary

To that end, this chapter discusses three foundational aspects of cyberspace as an operational domain and their relevance to the operational artist: the conceptualization of cyberspace as an operational domain, the nature of cyberspace as an operational domain, and the implications of cyberspace as an operational domain. Again, demonstrating that cultivation of a deeper understanding of cyberspace as an operational domain is within the grasp of the operational artist, and can be achieved through the deliberate development of cyberspace knowledge as it relates to operational art.

The first aspect of importance to the operational artist, the conceptualization of cyberspace as an operational domain, addresses the doctrinal characterization of cyberspace as a domain and the conceptual construct of the domain itself. Analyzing this construct provides the operational artist a foundation through which to view and understand the domain, recognizing the dependence of cyberspace on both the physical and human aspects of the domain, while also acknowledging the shortfalls in current cyberspace doctrine.

The second aspect highlighted in this chapter focuses on developing the operational artist's understanding of the nature of the cyberspace domain. Unlike the other physical domains, cyberspace was wholly created by man and, as such, man shapes the character of the cyberspace domain. Also unlike the air, land, sea, and space

domains, which have physical limitations in time and space, the cyberspace domain, unrestricted by the laws of physics, has transcended the traditional constructs of states and the physical limitations of geography, linking civilizations and societies in ways unprecedented in human history.

The third aspect examines the implications of cyberspace as an operational domain via three key elements: the operational space within the cyberspace domain, Department of Defense activities within the domain, and operations in and through cyberspace. The first element focuses on the three categories of operational space within the cyberspace domain: blue cyberspace (Department-of-Defense-protected cyberspace), red cyberspace (adversary-protected cyberspace), and gray cyberspace (utilized by friends, adversaries, states and individuals). The second element of the domain focuses on the Department of Defense activities conducted in cyberspace and their relationship to the blue, gray, and red cyberspace, while the third element, implications for the cyberspace domain, identifies the operational aspects of activities *in* cyberspace, operations *through* cyberspace, and activities *in* and *through* cyberspace.

Effectively employing cyberspace capabilities requires a sophisticated understanding of the three foundational aspects of cyberspace as an operational domain. The operational artist, armed with a cognitive understanding of cyberspace and its implications for the joint force commander, will underpin a comprehensive operational approach that magnifies effects in all domains.

CHAPTER THREE:

INTEGRATION OF CYBERSPACE INTO THE OPERATIONAL DESIGN

This chapter applies the understanding of cyberspace as an operational domain to operational art and design in terms of the imaginative integration and synchronization of cyberspace effects into the operational design process.

Joint Publications 5-0, *Joint Operations*, identifies 13 elements of operational design that can assist in military planning activities and can be drawn upon as appropriate, depending on the nature of the operation being developed.[1] Of the 13 elements of operational design, there are two that, in the context of the cyberspace domain, warrant thorough consideration: center(s) of gravity, and decisive points. These elements, while applicable to military operations in all domains, hold particular relevance within the cyberspace domain. For the operational artist, understanding these elements—in the context of cyberspace in the operational environment and as an operational domain—allows better synchronization of cross-domain operations, as well as unique cyberspace activities that can be employed in time and space to generate the desired effects and achieve operational objectives. In addition to these elements of operational design, the operational artist must also recognize the critical role authorities play in the application of cyberspace capabilities in the operational design.

In short, understanding center(s) of gravity, decisive points, and the role authorities play in the conduct of cyberspace operations allows the operational artist to employ cyberspace forces and effects decisively at the operational level of war.

---

[1] Office of the Chairman of the Joint Chiefs of Staff, *Joint Planning*, Joint Publication 5-0, (Washington, D.C.: The Joint Staff, 16 June 2017), pp. IV-6-IV-40.

Centers of Gravity

Carl Von Clausewitz described the center of gravity as "the hub of all power and movement, on which everything depends."[2] United States military doctrine echoes Clausewitz, stating that "a COG [center of gravity] is a source of power that provides moral or physical strength, freedom of action, or will to act."[3] Taken together, it becomes clear to the operational artist that he must identify and act on adversary centers of gravity in order to generate the desired effects within the operational environment in order to achieve desired ends.

The aspect of centers of gravity that warrants additional considerations in the context of the cyberspace domain is the direct, and arguably unimpeded, access to the citizenry of a state or social group that can be achieved by leveraging the cyberspace domain.[4] Cyberspace offers the opportunity to shape the socio-psychological aspects of a target audience directly, in ways that other domains cannot. Of note, cyberspace activities can generate effects in support of the physical domains, or function independently.

For the operational artist, this means that the center of gravity must be described in socio-psychological terms, as well as in traditional terms of physical composition so

---

[2] Clausewitz, *On War*, p. 720.
[3] Office of the Chairman of the Joint Chiefs of Staff, *Joint Planning*, p. IV-23.
[4] The concept of COGs existed long before man created the cyberspace domain; therefore, cyberspace should not alter the operational artist's understanding of what a COG is and isn't. However, some cyberspace theorists imagine the cyberspace domain to be a COG in and of itself, suggesting that cyberspace "exists solely as lines of communications" representing a "global center of gravity." This perception of cyberspace as a COG likely stems from Clausewitz's definition of COGs. However, this perspective is flawed. To propose that the cyberspace domain is a COG is likened to proposing that the land domain is a COG. The land is not the COG; what the control of the land *represents* is a COG, (e.g., a seat of government and therefore political power). Aucsmith, *A Theory of War in the Cyber Domain*, p. 17.

that cyberspace planners can target the center of gravity effectively. In some instances, cyberspace may be the only component that can influence an enemy center of gravity directly. Therefore, the analysis of the center of gravity must include a clear and unambiguous description of the social-psychological aspects of the adversary center of gravity. In the same manner, the desired end state must be described in socio-psychological terms for the cyberspace component to be able to plan and execute operations within the operational design that achieves the desired effects within the target audience, without generating unintended consequences, or perhaps never even initiating active combat.

In addition to recognizing opportunities to influence adversary centers of gravity through cyberspace activities, the operational artist must also recognize the vulnerabilities that cyberspace represents for joint force centers of gravity as well. While the day-to-day security of blue cyberspace is an ongoing activity, and can be easily taken for granted, the operational artist must look at the operations that are planned in the physical warfighting domains to ensure that cyberspace protection activities are initiated to ensure the availability of the critical cyberspace segments that enable these activities. Due to the nature and construct of cyberspace, cyberspace protection activities, similar to Julian Corbett's concept of sea power, must be planned and executed to ensure access to the required segments of cyberspace coordinated in time and space with the protected activities being conducted in the physical domain.[5]

---

[5] Julian Corbett, *Some Principles of Maritime Strategy*, (Breinigsville, PA: DODO Press, 2011), pp. 54-67; Springer, *Cyber Warfare*, pp. 64-66; Aucsmith, *A Theory of War in the Cyber Domain*, pp. 17-20.

Decisive Points

Joint Publication 5-0, *Joint Planning,* defines a decisive point as "a geographic place, specific key event, critical factor, or function that, when acted upon, allows . . . a marked advantage over an enemy or contribute[s] materially to achieving success."[6] Identifying decisive points that can be acted upon in and/or through the cyberspace domain requires that the operational artist have a deep understanding of the implications of the cyberspace domain on the operational environment. Decisive points must be closely analyzed to judge whether operationally-specific actions or results can be obtained through leveraging cyberspace capabilities. Once identified, the decisive points and the results desired from actions on those decisive points must be clearly defined in terms of time, space, and effect, and whether the effects should be permanent or temporary, destructive or disruptive.

These cyberspace activities must be synchronized in terms of time and effect with all other relevant components, and be communicated to the appropriate elements of the joint force to ensure unity of effort and enhance the overall effectiveness of the joint force through cross-domain combined arms maneuver. The tools presented in Chapter Two (Figures 2, 3, and 4), as well as the appendices of this paper, assist the operational artist in incorporating cyberspace capabilities into the operational design. In the contemporary operational environment, cyberspace operations are an essential line of operations in the operational design. To succeed in elevating the application of cyberspace capabilities in time and space to the level of operational art, the operational

[6] Office of the Chairman of the Joint Chiefs of Staff, *Joint Planning,* p. GL-8.

artist must deliberately integrate the cyberspace domain and its complementary relationship with operations and capabilities resident in the air, land, sea, and space domains.

Authorities

The operational artist must analyze the operational environment, define operational objectives, develop the operational approach, identify centers of gravity, designate decisive points, and establish lines of operation. Without the appropriate authorities, however, cyberspace operations will not achieve the desired effects, in time or space.

The operational artist may discover during the operational design process that success in the operational environment requires the application of information-related capabilities in and/or through the cyberspace domain. In these instances, the operational artist must determine if the desired effects qualify as a cyberspace activity or an information-related capability, or if the operation involves elements of both. Once the determination is made, the operational artist will coordinate with the appropriate entities to request the necessary authorities. Examples of additional authorities that may be required include authorities to conduct special technical operations (STO), or to release and execute sensitive information-related capabilities (IRC) against target audiences through the cyberspace domain.[7]

The operational artist must analyze the operational approach and associated lines of operation to determine what authorities are required to execute cyberspace operations in support of the campaign, concept, and operational plans. As Joint Publication 3-12,

[7] Office of the Chairman of the Joint Chiefs of Staff, *Information Operations*, pp. IV-1-IV-2.

Cyberspace Operations, indicates, "to plan for, authorize [refers to commander approval], and assess these actions [cyberspace activities], it is important the commander and staff clearly understand which actions have been authorized under their current mission order."[8] Second only to identifying the need for additional authorities to conduct cyberspace operations, the timing of the receipt of specific delegation for the necessary authorities is of critical importance, as a delay could render an entire line of operation combat ineffective. The operational artist must understand the essential importance of integrating operations in time and space for decisive effect. Therefore, the operational artist must plan and coordinate far in advance to obtain the required authorities through a detailed and thorough knowledge of the operational design.

Cyberspace and Operational Design: A Summary

Advancing the operational artist's conceptualization and application of cyberspace capabilities requires deliberate study and analysis of the cyberspace domain as it relates to operational art and design. Integration of the cyberspace into the operational design process is paramount in the contemporary operational environment, as is the deliberate development of knowledge as it relates to the employment of cyberspace capabilities at the operational level of war. Cyberspace not only presents new opportunities for the joint force to affect adversary centers of gravity, cyberspace also reveals the vulnerability of joint force centers of gravity and their associated critical capabilities and requirements, highlighting the need to protect access while we project effects in and through the cyberspace domain.

[8] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, p. II-5.

Cyberspace activities and their associated effects must be coordinated with other lines of operation in the operational approach to ensure joint force objectives are achieved. This requires the communication of intent across joint force components to enable synchronization of cross-domain operations in time, space, and effect to maximize operational utility while mitigating risk to the joint force. The operational artist must also understand cyberspace operations within the operational design in terms of enabling other information-related capabilities and their implications on authorities in the cyberspace domain. Building on the understanding of cyberspace integration into operational design and the resulting cyberspace line of operation within the operational approach, this chapter highlights the importance of obtaining the requisite authorities necessary for the commander to execute cyberspace operations at the operational level of war.

Ultimately, these efforts will result in a common point of departure for the application of cyberspace operations in time and space at the operational level of war to achieve operational, and strategic objectives, thereby balancing risk, and aligning ends, ways, and means to achieve the desired ends of the joint force commander.

CONCLUSION

Up to this point in history, the United States' application of cyber power and cyberspace capabilities has been technologically innovative but operationally unimaginative, primarily consisting of the strategic application of tactical capabilities with limited consideration for the integration of those capabilities at the operational level of war.[1] Cyberspace as a warfighting domain is grossly misunderstood by the majority of military planners and senior leaders.[2] The degree to which cyberspace and cyber power are misunderstood within the Department of Defense makes successful integration of cyberspace capabilities across the warfighting domains nearly impossible, with successes more closely resembling luck rather than design. In the contemporary global environment, where cyberspace is woven into the fabric of the interactions between actors, individuals, and states, those states that advance cyberspace to the operational level of war, and develop a common understanding of cyberspace as an operational domain, will have a decisive advantage in the contemporary, and future, operational environment.

Successful integration of cyberspace at the operational level of war relies on three elements: a revised concept and understanding of war and warfare as influenced by the cyberspace domain, the employment of cyberspace power as a strategic and operational construct, and the application of cyberspace activities within operational design and applied through the operational art. Taken as a whole, the Department of Defense must

---

[1] Nakesone, "A Cyber Force for Persistent Operations," p. 11.
[2] Illustrating this point, the *Washington Post* recently published an article that identified, and attempted to dispel, five myths associated with cyberspace. This demonstrates that misunderstanding related to cyberspace is prevalent in contemporary society. Ben Buchanan, "Five Myths: Cyberwar," *The Washington Post*, March 1, 2020.

develop a common understanding of cyberspace and cyberspace power. Without this common point of departure, it will be impossible to integrate cyberspace and cyberspace power across the warfighting domains, thereby making globally integrated operations impossible.

The inherently interlinked and interdependent nature of the cyberspace domain indicates how cyberspace has fundamentally altered the interactions between states, between states and individuals, and between social groups. The operational artist must, therefore, recognize the effects the cyberspace domain has on the doctrinal elements of operational design. Effectively employing cyberspace capabilities in support of United States national strategic ends requires not only a common understanding of cyberspace power, but a sophisticated understanding of cyberspace as an operational domain, and its relationship to the other operational domains of air, land, sea, and space.

This sophisticated understanding of cyberspace as an operational domain must—at a minimum—include an understanding of the implications of cyberspace on warfare in the contemporary environment, as an operational domain, and in operational design. Chapter One addresses the effects of cyberspace on the contemporary environment, focusing on the origins of cyberspace and its contemporary manifestation, the manifestation of threats in cyberspace, and the implications cyberspace has for the operational artist's understanding of war, warfare, and competition in the geo-strategic environment. Chapter Two discusses cyberspace as an operational domain, focusing on the construct of the cyberspace domain itself, the conceptualization of the operational space within the domain and Department of Defense activities within blue, gray, and red cyberspace, as well as the implications the elements of cyberspace hold for operational

art. Chapter Three demonstrates the need to conceptualize cyberspace in terms of operational design, focusing on the development of cyberspace understanding as it relates to centers of gravity, decisive points, and the authorities required to plan and execute cyberspace operations in and/or through the domain. Together, the elements of cyberspace as an operational domain described in this paper provide a basis of understanding, and a common point of departure from which the operational artist can begin to leverage United States Department of Defense cyberspace capabilities at the operational level of war.

Armed with this understanding of cyberspace as an operational domain, the operational artist can apply cyberspace power, using the operational design to synchronize and integrate operations across the air, land, sea, space, and cyberspace domains. The operational artist must demystify cyberspace power, recognize its operational and strategic utility, and employ capabilities in time and space for decisive effect, either singularly or in synchronization with, and through the integration of, other components in other domains, assembled and executed through the operational approach and executed through the operational art. This requires understanding of cyberspace as an operational domain, establishing a common point of departure for operational artists to ensure cyberspace capabilities are employed effectively across the operational domains and at the appropriate levels of war.

EPILOGUE

Returning to the vignette that opened this discussion on the cyberspace domain, now, with a common point of departure established for understanding cyberspace at the operational level of war, we can begin to see how the meeting may have gone very differently.

A meeting was held in one of the many small, non-descript conference rooms scattered across the National Capital Region to discuss plans and operations for one of the many Joint Task Forces (JTF) active at the time. The team included representatives from the task force's operations and planning elements, Department of Defense organizations, and inter-agency partners. The JTF representatives described their mission and the strategic ends toward which the JTF was working. At a point in the discussions, the lead operations planner for the JTF indicated that the integration of cyberspace activities—in coordination with other cross-domain operations—was being considered as a means through which the JTF could achieve the desired strategic end-state.

The JTF planner then presented a cyberspace line of operation, nested within the larger operational approach, an approach that had been previously developed for, and approved by, the responsible commander. The cyberspace line of operation was integrated with other complementary lines of operation, and the planner was able to clearly describe the decisive points that his team felt could be achieved via Department of Defense activities conducted in and through the cyberspace domain in terms of time, space, and effects. This generated numerous questions, the majority of which were related to understanding the appropriateness of some of the critical vulnerabilities related to the decisive points, as well as the risks associated with, and authorities required to

execute, the operations as described by the planning team. These discussions confirmed many of the planning team's assessments and, recognizing that operational design is an iterative process, generated questions and identified factors that required further investigation for others. The team adjourned, setting additional coordination meetings to advance the operational approach and support continued course of action development and planning efforts.

The attendees—having a common understanding of cyberspace as an operational domain—were able to analyze and refine the cyberspace line of operation to support achievement of the stated strategic, operational, and tactical level objectives in time and space, thereby balancing risk, identifying necessary authorities, and aligning ends, ways, and means to achieve desired ends of the joint force commander.

APPENDICES

Appendix 1: Cyberspace Mission Forces and Activities

The matrix below was generated by the author and captures the five Department of Defense cyberspace activities as they relate to the department of defense cyberspace mission forces. The intent of this matrix is to provide the operational artist a tool through which he can conceptualize Department of Defense cyberspace activities and the forces that execute those activities. (Note: Derived from *Cyberspace Operations*, Joint Publication 3-12; in Chapter Two, a derivative of the matrix is identified as Figure 3.)

		Cyberspace Mission Forces					
Cyberspace Activities[1]		Cyberspace Protection Team (CPT)	Combat Mission Team (CMT)	Combat Support Team (CST)	National Mission Team (NMT)	National Support Team (NST)	Mission-Tailored Force Package (MTFP)
Cyberspace Security	DoDIN[2]						
	Other[3]						
Cyberspace Defense	Internal Cyberspace[4]						
	External Cyberspace[5]						
Cyberspace Countermeasures[6]	OCO[7]						
	DCO[8]						
Cyberspace Exploitation[9]	Intelligence[10, 11]						
	Maneuver[12]						
Cyberspace Attack[13]	Nonlethal Fires (Manipulate)[14]						
	Lethal Fires (Destroy)[15]						

Notes:
i. Cyber Protection Force (CPF): The CPF conducts cyberspace operations (CO) for internal protection of the DoDIN or other blue cyberspace when ordered. The CPF consists of cyberspace protection teams (CPTs) organized, trained, and equipped to defend assigned cyberspace. (Green blocks)
ii. Cyber National Mission Force (CNMF): The CNMF conducts CO to defeat cyberspace threats to the DODIN and, when ordered, to the nation. The CNMF consists of national mission teams (NMTs), associated national support teams (NSTs), and national-level CPTs for protection of non-DoDIN blue cyberspace. (Blue blocks)
iii. Cyber Combat Mission Force (CCMF): The CCMF conducts CO to support the missions, plans, and priorities of the geographic and functional combatant commanders (CCDRs). The CCMF is comprised of combat mission teams (CMTs) and associated combat support teams (CSTs). (Orange blocks)
iv. When directed, USCYBERCOM establishes a tailored force to support specific comatatant command (CCMD) crisis or contingency mission requirements beyond the capacity of forces available for routine support; mission-tailored force packages (MTFPs) are task-organized and support CCDR for the duration of the crisis/contingency or until redeployed by CDRUSCYBERCOM in coordination with the supported CCDR (CCDR has tactical contol (TACON) to control the timing and tempo of cyberspace operations). (Purple blocks)

Footnotes:
1. DoD cyberspace operations are divided into three categories spanning five activities: DoDIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).
2. DoDIN encompasses all DoD information networks.
3. Non-DoD segments of cyberspace the DoD has been directed to protect.
4. DoD-protected cyberspace; authority to conduct DCO within protected cyberspace reside with the designated CCMD authority; encompasses Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IM).
5. Gray and red cyberspace; designated commander may require additional authorities to conduct defensive operations outside DoD-protected cyberspace; encompasses Defensive Cyberspace Operations-Response Actions (DCO-RA).
6. Cyberspace activities that focus on the impairment of the operational effectiveness of enemy activity.
7. DoD actions in or through gray and red cyberspace to negate adversary activities and capabilities.
8. DoD defensive actions in blue, gray, and red cyberspace to interdict or mitigate adversary activities or capabilities; defensive actions are normally nondestructive or nonlethal in nature.
9. DoD activities in gray and red cyberspace that do not generate attack effects.
10. Supports current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value.
11. Cyberspace intelligence, surveillance, and reconnaissance (ISR) activities are included in cyberspace exploitation activities and are focused on gathering tactical and operational information and on mapping adversary cyberspace segments to support military planning.
12. Non-attack activities in gray and red cyberspace to facilitate gaining access to adversary, enemy, or intermediary links and nodes; shaping the cyberspace domain to support future actions.
13. DoD activities (fires) in gray and red cyberspace that generate attack effects (deny, degrade, disrupt, destroy, neutralize, etc.) in cyberspace or other domains; fires should be discussed in terms of target, method, and effect.
14. This category of fires uses an adversary's information resources for friendly purposes to create denial effects not immediately apparent in cyberspace.
15. This category of fires generates overt effects that will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.

Derived from Joint Publication 3-12, *Cyberspace Operations* , 8 June 2018.

Matrix 1: Cyberspace Mission Force and Cyberspace Activities

Appendix 2: Cyberspace Activities and Joint Functions

The matrix below was generated by the author and captures the five Department of Defense cyberspace activities as they relate to the seven functions of the Joint Force. The intent of this matrix is to provide the operational artist a tool through which he can conceptualize the cyberspace domain and its application in support of the seven warfighting functions and the joint force. (Note: The matrix was derived from *Cyberspace Operations*, Joint Publication 3-12, and *Joint Operations*, Joint Publication 3-0.)

	Cyberspace Activities									
Joint Functions	Cyberspace Security		Cyberspace Defense		Cyberspace Countermeasures		Cyberspace Exploitation		Cyberspace Attack	
	DoDIN[2]	Other[3]	Internal Cyberspace[4]	External Cyberspace[5]	OCO[7]	DCO[8]	Intelligence[10, 11]	Maneuver[12]	Nonlethal Fires (Manipulate)[14]	Lethal Fires (Destroy)[15]
Command & Control										
Information										
Intelligence										
Fires										
Movement & Maneuver										
Protection										
Sustainment										

Notes:
i. Cyberspace activities should be assessed and implemented in the context of operational objectives, centers of gravity (COGs), decisive points, and tasks, and in concert with activities across the air, land, sea, and space warfighting domains to maximize effectiveness of joint force operations.
ii. Under certain conditions, however limited, cyberspace capabilities may be employed independent of adjoining activities in other warfighting domains; all cyberspace activities must be planned and assessed in terms of the ability of the activity to achieve the desired effect and any potential secondary effects that could be generated by the activity as well as the effect the activity may have on other joint force activities.
iii. Approval for cyberspace operations (CO) in gray and red cyberspace requires separate authorities from those that authorize CO in blue cyberspace; the required authorizations may be held by the joint force commander, or they may be held at a higher level of command. Planners must identify and request (if the authorities are not already delegated to the joint force commander) the authorities and forces necessary to execute operationally relevant CO.
iv. Cyberspace defense and cyberspace countermeasures can be offensive or defensive in nature, dependent upon the intended effect of the action.

Footnotes:
1. DoD cyberspace operations are divided into three categories spanning five activities: DoDIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).
2. DoDIN encompasses all DoD information networks.
3. Non-DoD segments of cyberspace the DoD has been directed to protect.
4. DoD-protected cyberspace; authority to conduct DCO within protected cyberspace reside with the designated CCMD authority; encompasses Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IM).
5. Gray and red cyberspace; designated commander may require additional authorities to conduct defensive operations outside DoD-protected cyberspace; encompasses Defensive Cyberspace Operations-Response Actions (DCO-RA).
6. Cyberspace activities that focus on the impairment of the operational effectiveness of enemy activity.
7. DoD actions in or through gray and red cyberspace to negate adversary activities and capabilities.
8. DoD defensive actions in blue, gray, and red cyberspace to interdict or mitigate adversary activities or capabilities; defensive actions are normally nondestructive or nonlethal in nature.
9. DoD activities in gray and red cyberspace that do not generate attack effects.
10. Supports current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value.
11. Cyberspace intelligence, surveillance, and reconnaissance (ISR) activities are included in cyberspace exploitation activities and are focused on gathering tactical and operational information and on mapping adversary cyberspace segments to support military planning.
12. Non-attack activities in gray and red cyberspace to facilitate gaining access to adversary, enemy, or intermediary links and nodes; shaping the cyberspace domain to support future actions.
13. DoD activities (fires) in gray and red cyberspace that generate attack effects (deny, degrade, disrupt, destroy, neutralize, etc.) in cyberspace or other domains; fires should be discussed in terms of target, method, and effect.
14. This category of fires uses an adversary's information resources for friendly purposes to create denial effects not immediately apparent in cyberspace.
15. This category of fires generates overt effects that will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.

Derived from Joint Publication 3-12, *Cyberspace Operations,* 8 June 2018, and Joint Publication 3-0, *Joint Operations,* 22 October 2018.

Matrix 2: Cyberspace Activities and the Joint Warfighting Functions

Appendix 3: Cyberspace Activities and the Joint Force

The matrix below was generated by the author and captures the five Department of Defense cyberspace activities as they relate to the elements of the Joint Force. The intent of this matrix is to provide the operational artist a tool through which he can conceptualized the cyberspace domain and its application to cross-domain operations and the joint force. (Note: The matrix was derived from *Cyberspace Operations*, Joint Publication 3-12 and *Joint Planning*, Joint Publication 5-0*;* in Chapter Two, a derivative of this matrix is identified as Figure 4.)

	Cyberspace Activities									
Joint Force Elements	Cyberspace Security		Cyberspace Defense		Cyberspace Countermeasures		Cyberspace Exploitation		Cyberspace Attack	
	DoDIN[2]	Other[3]	Internal Cyberspace[4]	External Cyberspace[5]	OCO[7]	DCO[8]	Intelligence[10, 11]	Maneuver[12]	Nonlethal Fires (Manipulate)[14]	Lethal Fires (Destroy)[15]
Air Component										
Land Component										
Maritime Component										
Space Component										
Special Operations Component										
Inter-Agency										
Non-U.S. Partner										

Notes:
i. Cyberspace activities should be assessed and implemented in the context of operational objectives, centers of gravity (COGs), decisive points, and tasks, and in concert with activities across the air, land, sea, and space warfighting domains to maximize effectiveness of joint force operations.
ii. Under certain conditions, however limited, cyberspace capabilities may be employed independent of adjoining activities in other warfighting domains; all cyberspace activities must be planned and assessed in terms of the ability of the activity to achieve the desired effect and any potential secondary effects that could be generated by the activity as well as the effect the activity may have on other joint force activities.
iii. Approval for cyberspace operations (CO) in gray and red cyberspace requires separate authorities from those that authorize CO in blue cyberspace; the required authorizations may be held by the joint force commander, or they may be held at a higher level of command. Planners must identify and request (if the authorities are not already delegated to the joint force commander) the authorities and forces necessary to execute operationally relevant CO.
iv. Cyberspace defense and cyberspace countermeasures can be offensive or defensive in nature, dependent upon the intended effect of the action.

Footnotes:
1. DoD cyberspace operations are divided into three categories spanning five activities: DoDIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).
2. DoDIN encompasses all DoD information networks.
3. Non-DoD segments of cyberspace the DoD has been directed to protect.
4. DoD-protected cyberspace; authority to conduct DCO within protected cyberspace reside with the designated CCMD authority; encompasses Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IM).
5. Gray and red cyberspace; designated commander may require additional authorities to conduct defensive operations outside DoD-protected cyberspace; encompasses Defensive Cyberspace Operations-Response Actions (DCO-RA).
6. Cyberspace activities that focus on the impairment of the operational effectiveness of enemy activity.
7. DoD actions in or through gray and red cyberspace to negate adversary activities and capabilities.
8. DoD defensive actions in blue, gray, and red cyberspace to interdict or mitigate adversary activities or capabilities; defensive actions are normally nondestructive or nonlethal in nature.
9. DoD activities in gray and red cyberspace that do not generate attack effects.
10. Supports current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value.
11. Cyberspace intelligence, surveillance, and reconnaissance (ISR) activities are included in cyberspace exploitation activities and are focused on gathering tactical and operational information and on mapping adversary cyberspace segments to support military planning.
12. Non-attack activities in gray and red cyberspace to facilitate gaining access to adversary, enemy, or intermediary links and nodes; shaping the cyberspace domain to support future actions.
13. DoD activities (fires) in gray and red cyberspace that generate attack effects (deny, degrade, disrupt, destroy, neutralize, etc.) in cyberspace or other domains; fires should be discussed in terms of target, method, and effect.
14. This category of fires uses an adversary's information resources for friendly purposes to create denial effects not immediately apparent in cyberspace.
15. This category of fires generates overt effects that will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.

Derived from Joint Publication 3-12, *Cyberspace Operations* , 8 June 2018.

Matrix 3: Cyberspace Activities and the Joint Force

Appendix 4: Cyberspace Activities and Operational Approach

The matrices below were generated by the author and capture the five Department of Defense cyberspace activities as they relate to the operational approach (Matrix 1 depicts a three-phase approach, Matrix 2 depicts a five-phase approach). The intent of these matrixes is to provide the operational artist a tool through which he can conceptualize the cyberspace domain and its application in time, space, and effect to advance understanding of how cyberspace capabilities can be applied throughout the operational approach. (Note: The matrices were derived from *Cyberspace Operations*, Joint Publication 3-12.)

		Operational Approach		
Cyberspace Activities[1]		PHASE I: Deter	PHASE II: Defeat	PHASE III: Redeploy
Cyberspace Security	DoDIN[2]			
	Other[3]			
Cyberspace Defense	Internal Cyberspace[4]			
	External Cyberspace[5]			
Cyberspace Countermeasures[6]	OCO[7]			
	DCO[8]			
Cyberspace Exploitation[9]	Intelligence[10, 11]			
	Maneuver[12]			
Cyberspace Attack[13]	Nonlethal Fires (Manipulate)[14]			
	Lethal Fires (Destroy)[15]			

Notes:
i. Cyberspace activities should be assessed and implemented in the context of operational objectives, centers of gravity (COGs), decisive points, and tasks, and in concert with activities across the air, land, sea, and space warfighting domains to maximize effectiveness of joint force operations.
ii. Under certain conditions, however limited, cyberspace capabilities may be employed independent of adjoining activities in other warfighting domains; all cyberspace activities must be planned and assessed in terms of the ability of the activity to achieve the desired effect and any potential secondary effects that could be generated by the activity as well as the effect the activity may have on other joint force activities.
iii. Approval for cyberspace operations (CO) in gray and red cyberspace requires separate authorities from those that authorize CO in blue cyberspace; the required authorizations may be held by the joint force commander, or they may be held at a higher level of command. Planners must identify and request (if the authorities are not already delegated to the joint force commander) the authorities and forces necessary to execute operationally relevant CO.
iv. Cyberspace defense and cyberspace countermeasures can be offensive or defensive in nature, dependent upon the intended effect of the action.

Footnotes:
1. DoD cyberspace operations are divided into three categories spanning five activities: DoDIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).
2. DoDIN encompasses all DoD information networks.
3. Non-DoD segments of cyberspace the DoD has been directed to protect.
4. DoD-protected cyberspace; authority to conduct DCO within protected cyberspace reside with the designated CCMD authority; encompasses Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IM).
5. Gray and red cyberspace; designated commander may require additional authorities to conduct defensive operations outside DoD-protected cyberspace; encompasses Defensive Cyberspace Operations-Response Actions (DCO-RA).
6. Cyberspace activities that focus on the impairment of the operational effectiveness of enemy activity.
7. DoD actions in or through gray and red cyberspace to negate adversary activities and capabilities.
8. DoD defensive actions in blue, gray, and red cyberspace to interdict or mitigate adversary activities or capabilities; defensive actions are normally nondestructive or nonlethal in nature.
9. DoD activities in gray and red cyberspace that do not generate attack effects.
10. Supports current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value.
11. Cyberspace intelligence, surveillance, and reconnaissance (ISR) activities are included in cyberspace exploitation activities and are focused on gathering tactical and operational information and on mapping adversary cyberspace segments to support military planning.
12. Non-attack activities in gray and red cyberspace to facilitate gaining access to adversary, enemy, or intermediary links and nodes; shaping the cyberspace domain to support future actions.
13. DoD activities (fires) in gray and red cyberspace that generate attack effects (deny, degrade, disrupt, destroy, neutralize, etc.) in cyberspace or other domains; fires should be discussed in terms of target, method, and effect.
14. This category of fires uses an adversary's information resources for friendly purposes to create denial effects not immediately apparent in cyberspace.
15. This category of fires generates overt effects that will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.

Derived from Joint Publication 3-12, *Cyberspace Operations,* 8 June 2018.

Matrix 4: Cyberspace Activities and the Operational Approach (Three Phases)

		Operational Approach				
Cyberspace Activities[1]		PHASE I: Shape	PHASE II: Deter & Posture	PHASE III: Respond & Defeat	PHASE IV: Stabilize	PHASE V: Transition to Civial Authority
Cyberspace Security	DoDIN[2]					
	Other[3]					
Cyberspace Defense	Internal Cyberspace[4]					
	External Cyberspace[5]					
Cyberspace Countermeasures[6]	OCO[7]					
	DCO[8]					
Cyberspace Exploitation[9]	Intelligence[10, 11]					
	Maneuver[12]					
Cyberspace Attack[13]	Nonlethal Fires (Manipulate)[14]					
	Lethal Fires (Destroy)[15]					

Notes:
i. Cyberspace activities should be assessed and implemented in the context of operational objectives, centers of gravity (COGs), decisive points, and tasks, and in concert with activities across the air, land, sea, and space warfighting domains to maximize effectiveness of joint force operations.
ii. Under certain conditions, however limited, cyberspace capabilities may be employed independent of adjoining activities in other warfighting domains; all cyberspace activities must be planned and assessed in terms of the ability of the activity to achieve the desired effect and any potential secondary effects that could be generated by the activity as well as the effect the activity may have on other joint force activities.
iii. Approval for cyberspace operations (CO) in gray and red cyberspace requires separate authorities from those that authorize CO in blue cyberspace; the required authorizations may be held by the joint force commander, or they may be held at a higher level of command. Planners must identify and request (if the authorities are not already delegated to the joint force commander) the authorities and forces necessary to execute operationally relevant CO.
iv. Cyberspace defense and cyberspace countermeasures can be offensive or defensive in nature, dependent upon the intended effect of the action.

Footnotes:
1. DoD cyberspace operations are divided into three categories spanning five activities: DoDIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).
2. DoDIN encompasses all DoD information networks.
3. Non-DoD segments of cyberspace the DoD has been directed to protect.
4. DoD-protected cyberspace; authority to conduct DCO within protected cyberspace reside with the designated CCMD authority; encompasses Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IM).
5. Gray and red cyberspace; designated commander may require additional authorities to conduct defensive operations outside DoD-protected cyberspace; encompasses Defensive Cyberspace Operations-Response Actions (DCO-RA).
6. Cyberspace activities that focus on the impairment of the operational effectiveness of enemy activity.
7. DoD actions in or through gray and red cyberspace to negate adversary activities and capabilities.
8. DoD defensive actions in blue, gray, and red cyberspace to interdict or mitigate adversary activities or capabilities; defensive actions are normally nondestructive or nonlethal in nature.
9. DoD activities in gray and red cyberspace that do not generate attack effects.
10. Supports current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value.
11. Cyberspace intelligence, surveillance, and reconnaissance (ISR) activities are included in cyberspace exploitation activities and are focused on gathering tactical and operational information and on mapping adversary cyberspace segments to support military planning.
12. Non-attack activities in gray and red cyberspace to facilitate gaining access to adversary, enemy, or intermediary links and nodes; shaping the cyberspace domain to support future actions.
13. DoD activities (fires) in gray and red cyberspace that generate attack effects (deny, degrade, disrupt, destroy, neutralize, etc.) in cyberspace or other domains; fires should be discussed in terms of target, method, and effect.
14. This category of fires uses an adversary's information resources for friendly purposes to create denial effects not immediately apparent in cyberspace.
15. This category of fires generates overt effects that will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.

Derived from Joint Publication 3-12, *Cyberspace Operations*, 8 June 2018.

Matrix 5: Cyberspace Activities and the Operational Approach (Five Phases)

Appendix 5: U.S. Department of Defense Activities in Cyberspace

The graphic below was generated by the author and depicts the five types of cyberspace activities conducted by the Department of Defense, as well as their respective interactions with blue, gray, and red cyberspace. (The representation was derived from *Cyberspace Operations*, Joint Publication 3-12, and was modeled after a similar depiction of cyberspace as presented in the Marine Corps Cyberspace Warfare Group Command Brief, accessed 17 February 2020; in Chapter Two, this figure is identified as Figure 2.)

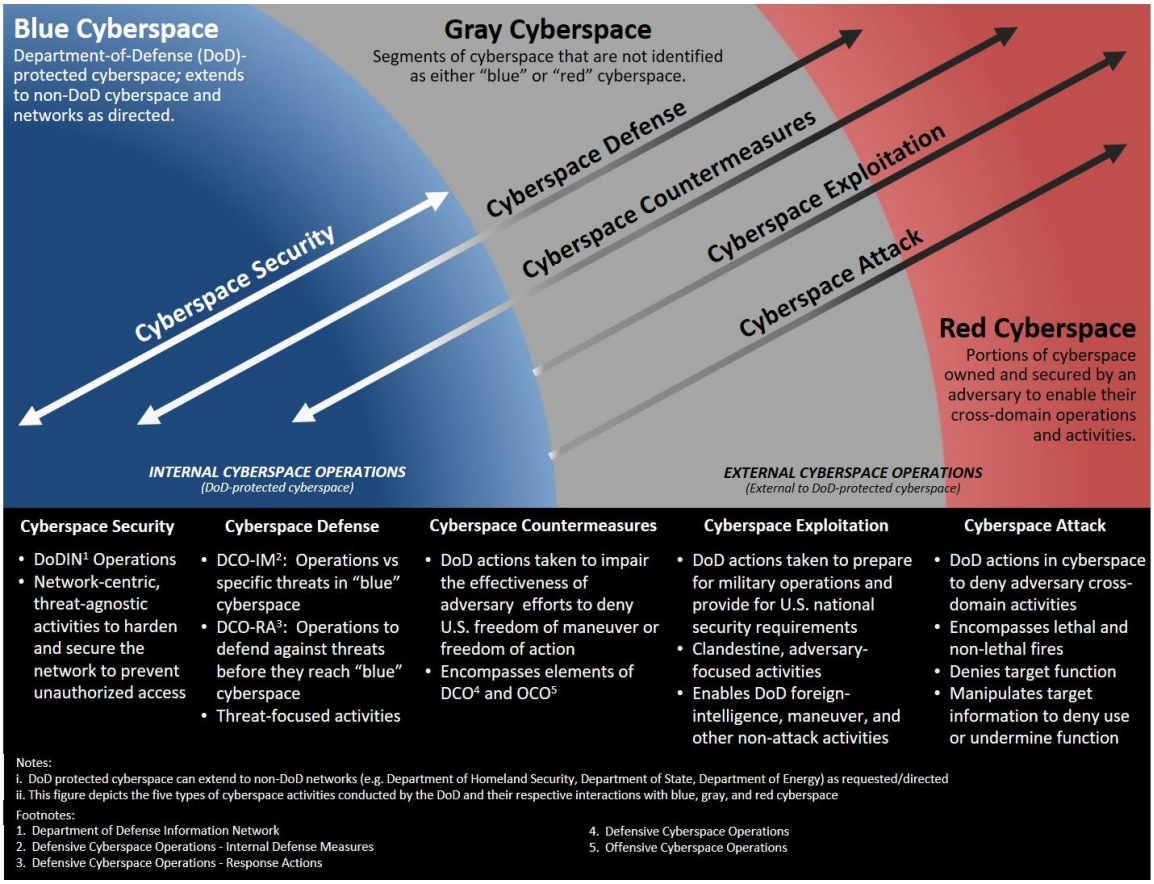


Figure 1: United States Department of Defense Cyberspace Activities

Appendix 6: Glossary

Part I—Acronyms

AFB	Air Force Base
ARPANET	Advanced Research
CCDR	Combatant Commander
CCMD	Combatant Command
CCMF	Cyber Combat Mission Force
CMF	Cyberspace Mission Force
CMT	Combat Mission Team
CNMF	Cyber National Mission Force
CO	Cyberspace Operations
COG	Center of Gravity
CPF	Cyber Protection Force
CPT	Cyberspace Protection Team
CST	Combat Support Team
DCO	Defensive Cyberspace Operations
DCO-IM	Defensive Cyberspace Operations-Internal Defense Measures
DCO-RA	Defensive Cyberspace Operations-Response Actions
DoD	Department of Defense
DoDIN	Department of Defense Information Network
EU	European Union
FBI	Federal Bureau of Investigation
FoA	Freedom of Action
FoM	Freedom of Maneuver
IADS	Integrated Air Defense System
IRC	Information-Related Capability
ISIL	Islamic State of Iraq and the Levant
ISR	Intelligence, Surveillance, and Reconnaissance
JP	Joint Publication

JTF	Joint Task Force
MTFP	Mission Tailored Force Package
NCR	National Capital Region
NMT	National Mission Team
NST	National Support Team
OCO	Offensive Cyberspace Operations
STO	Special Technical Operation
TACON	Tactical Control
TCP/IP	Transmission Control Protocol/Internet Protocol

Part II--Definitions

Cognitive Understanding. Comprehension, perception, and analytical ability acquired through the deliberate cultivation of knowledge to inform one's understanding of a given topic, environment, system, or situation. (As defined by the author.)

Cyber-persona Layer. "A view of cyberspace created by abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated, and their relationships to one another . . . the aggregate of an individual's or group's online identity(ies), and an abstraction of logical network layer data."[1]

Cyber Power. The "part of war that incorporates both the control and the use of information to influence the will of the people, not limited to the parties of the dispute."[2]

Cyberspace. "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3]

Cyber War. The "part of war that incorporates both the control and the use of information to influence the will of the people, not limited to the parties of the dispute."[4]

Cyberwar. "Conducting, and preparing to conduct, military operations according to information-related principles . . . disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself . . . turning the 'balance of information and knowledge' in one's favor, especially if the balance of forces is not . . . using knowledge so that less capital and labor may have to be expended." [5]

Cyberspace Warfare. Cyberspace activities encompassing all aspects of military, or para-military, operations normally conducted during wars or conflict among states, sub-states, and non-state actors, to advance an actor's interests while degrading, denying, destroying, influencing, or neutralizing an adversary's ability to do the same. (As defined by the author.)

Great Power Competition. Great power competition is the series of interactions between internationally recognized political entities possessing a combination of global economic, global military, or global political influence or capability to

---

[1] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, pp. I-4, IV-9.
[2] Poindexter, *The New Cyberwar: Technology and the Redefinition of Warfare*, p. 5.
[3] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, p. GL-4.
[4] Poindexter, *The New Cyberwar: Technology and the Redefinition of Warfare*, p. 5.
[5] Arquilla and Ronfeldt, "Cyberwar Is Coming!," p. 30.

either gain or maintain geo-strategic advantage while denying, degrading, or neutralizing a competitor's ability to do the same. (As defined by the author.)

Logical Network Layer. "Those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components . . . often represented through a network address (e.g., IP address) . . . [depicting] how nodes in the physical domains address and refer to one another to form entities in cyberspace . . . [this] is the first point where the connection to the physical domains may be lost."[6]

Netwar. "Information-related conflict at a grand level between nations and societies . . . [to] disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it." [7]

Physical-network Layer. "The IT [information technology] devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components . . . [and] includes wired (e.g., land and undersea cable) and wireless (e.g., radio, radio-relay, cellular, satellite) transmission means . . . it is a point of reference for determining geographic location."[8]

War. The application of violence by an organized group to influence the environment in pursuit of political objectives, legitimized by the group's constituency, and at all times influenced by their respective perception of their environment. (As defined by the author.)

Warfare. Activities encompassing all aspects of military, or para-military, operations normally conducted during wars or conflict among states, sub-states, and non-state actors, to advance an actor's interests while degrading, denying, destroying, influencing, or neutralizing an adversary's ability to do the same. (As defined by the author.)

---

[6] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, pp. I-3, I-4, IV-9.
[7] Arquilla and Ronfeldt, "Cyberwar Is Coming!," p. 28.
[8] Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, pp. I-2, I-3, IV-9.

BIBLIOGRAPHY

Arquilla, John and Ronfeldt, David. "Cyberwar Is Coming!," in *In Athena's Camp: Preparing for Conflict in the Information Age*, 23-60. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corporation, 1997.

Aucsmith, David. *A Theory of War in the Cyber Domain: Part 1, An Historical Perspective.* Microsoft Institute for Advanced Technology in Governments, 5 March 2012.

Carlin, John P. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. Edited by Garrett M. Graff. New York, NY: Public Affairs, 2018.

Clausewitz, Carl Von. *On War*. New York: Everyman's Library, 1993.

Corbett, Julian. *Some Principles of Maritime Strategy*. Breinigsville, PA: DODO Press, 2011.

Egloff, Florian. "Cybersecurity and the Age of Privateering," in *Understanding Cyber Conflict: 14 Analogies,* 231-247. Edited by George Perkovich and Ariel E. Levite. Washington, D.C.: Georgetown University Press, 2017.

Fidler, David P. "Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 71-87. Edited by Derek S. Reveron. Washington, D.C.: Georgetown University Press, 2012.

Fortune Business Insights. "Cyber Market Size, Share & Industry Analysis, 2019 – 2026." *Fortunebusinessinsights.com*. February 2020. (Report ID: FBI101165). https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 (accessed March 15, 2020).

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.

Kaldor, Mary. "Inconclusive Wars: Is Clausewitz Still Relevant in These Global Times?" *Global Policy*, Volume 3, Issue 10 (October 2010): 271-281.

Kaldor, Mary. *New and Old Wars: Organized Violence in a Global Era,* 3rd Edition. Stanford: Polity Press, 2012.

Kello, Lucas. *The Virtual Weapon and International Order*, New Haven: Yale University Press, 2017.

Lo, Bobo. *Russia and the New World Disorder*. Washington, D.C.: Brookings Institute Press, 2016.

Mishra, Lalit V. *Understanding Information Warfare: All You Need to Know.* Alpha Edition, 2017.

Munkler, Herfried. *The New Wars*. Cambridge, UK: Polity Press, 2005.

Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Forces Quarterly,* Vol. 92 (1st Quarter 2019): 10-14.

Nakasone, Paul M. "An Interview with Paul M. Nakasone." *Joint Forces Quarterly,* Vol. 92 (1st Quarter 2019): 4-9.

Office of the Chairman of the Joint Chiefs of Staff, Cyberspace Operations. Joint Publication 3-12. Washington, D.C.: The Joint Staff, 8 June 2018.

Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: The Joint Staff, January 2020.

Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication 3-13. Washington, D.C.: The Joint Staff, 20 November 2014.

Office of the Chairman of the Joint Chiefs of Staff, *Joint Fires*. Joint Publication 3-09. Washington, D.C.: The Joint Staff, 10 April 2019.

Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington, D.C.: The Joint Staff, 17 January 2017.

Office of the Chairman of the Joint Chiefs of Staff. *Joint Planning*. Joint Publication 5-0. Washington, D.C.: The Joint Staff, 16 June 2017.

Office of the Joint Chiefs of Staff. *Joint Task Force Headquarter*s. Joint Publication 3-33. Washington, D.C.: The Joint Staff, 31 January 2018.

Poindexter, Dennis F. *The New Cyberwar: Technology and the Redefinition of Warfare.* North Carolina: McFarland & Company, 2015.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Massachusetts: Massachusetts Institute of Technology, 2001.

Reveron, Derek S. "An Introduction to National Security and Cyberspace" in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 3-19. Edited by Derek S. Reveron. Washington, D.C.: Georgetown University Press, 2012.

Sheldon, John B. "Toward a Theory of Cyber Power," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 207-224. Edited by Derek S. Reveron. Georgetown University Press, Washington, D.C. 2012.

Springer, Paul J. Cyber Warfare. Santa Barbara, CA: ABC-CLIO, 2015.

Springer, Paul J. Encyclopedia of Cyber Warfare. Santa Barbara, CA: ABC-CLIO, 2017.

Trump, Donald J. *National Security Strategy of the United States of America.* Washington, D.C.: Government Printing Office, December 2017.

U.S. Department of Defense. Office of the Secretary of Defense. *The Department of Defense Cyber Strategy* 2015. By the Secretary of Defense. U.S. Department of Defense. Washington, D.C., 2015.

U.S. Department of Defense. Office of the Secretary of Defense. *2018 Department of Defense Cyber Strategy*, by the Secretary of Defense. U.S. Department of Defense. Washington, D.C., 2018.

Wood, Elizabeth A., Pomeranz, William E., Merry, E. Wayne, and Trudolyubov, Maxim. *Roots of Russia's War in Ukraine*. New York: Columbia University Press, 2016.

VITA

Lieutenant Colonel Ronnie B. Young is a career Intelligence Officer in the United States Air Force with experience in intelligence analysis, ISR operations, collection management, airbase defense, and special operations. Prior to attending the Joint Advanced Warfighting School (JAWS), Lt Col Young served as Deputy Commander, 707th Intelligence, Surveillance, and Reconnaissance Group, 70th Intelligence, Surveillance, and Reconnaissance Wing, Fort George G. Meade, Maryland, where he was responsible for integrating Air Force capabilities into global cryptologic operations, directly supporting national-level decision makers, combatant commanders, and tactical warfighters. Prior to Deputy, Group Command, Lt Col Young served as Commander, 34 Intelligence Squadron, supporting national, combatant command, and service requirements. Lt Col Young entered the Air Force in 2000 through the ROTC program at the University of Florida, Gainesville, Florida. He has served in positions at the squadron, group, wing, numbered air force, major command, air staff, joint, and coalition levels. Lt Col Young's academic credentials include a Master of Science in Defense Analysis (Irregular Warfare), a Master of Science in Management (Program Management), and a Bachelor of Arts in Political Science. He is a graduate of Naval Postgraduate School, University of Management and Technology, Air Command and Staff College, Squadron Officer School, Air Force Special Operations Command – Intelligence Formal Training Unit, Air Force Intelligence Officer Training, and Air and Space Basic Course.