SPECIAL WARFARE IN AND THROUGH CYBERSPACE: SHAPING THE OPERATIONAL ENVIRONMENT IN THE HUMAN DOMAIN

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

CHAD A. BARNES, MAJOR, UNITED STATES ARMY
B.S., Tennessee Technological University, Cookeville, Tennessee, 2006

Fort Leavenworth, Kansas
2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09-06-2017	Master's Thesis	AUG 2016 – JUN 2017

4. TITLE AND SUBTITLE

Special Warfare in and through Cyberspace: Shaping the Operational Environment in the Human Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Chad A. Barnes, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG 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

14. ABSTRACT

USSOCOM's contribution to unified land operations is through USASOC's critical capabilities of Special Warfare and Surgical Strike. Special warfare is unique in its reliance on indigenous war fighting capacity to stabilize or destabilize operational environments. Special Warfare, as a critical capability, and the conceptual application of special warfare in and through cyberspace must address special warfare's contribution to operational art in the human domain. This study uses a qualitative content analysis to explore the linkages between special warfare operations and cyberspace operations to support joint force commanders and U.S. embassy country teams in shaping the human domain. Further, cyber-enabled special warfare is explored through a typology of human action as a framework of analysis to develop methods of integrating cyberspace operations and special warfare.

15. SUBJECT TERMS
Special Warfare, cyberspace operations, cyber-enabled special warfare, human domain, Unconventional Warfare (UW), Foreign Internal Defense (FID), cyber electromagnetic activities (CEMA)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	74	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Chad A. Barnes

Thesis Title: Special Warfare in and through Cyberspace: Shaping the Operational Environment in the Human Domain

Approved by:

_____, Thesis Committee Chair
LTC Benjamin C. Croom, M.A.

_____, Member
Victor J. Delacruz, D.B.A.

_____, Member
LTC Paul M. Zeps, M.B.A.

Accepted this 9th day of June 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SPECIAL WARFARE IN AND THROUGH CYBERSPACE: SHAPING THE OPERATIONAL ENVIRONMENT IN THE HUMAN DOMAIN, by MAJ Chad A. Barnes, 74 pages.

United States Special Operations Command's contribution to unified land operations is through United States Army Special Operations Command's critical capabilities of special warfare and surgical strike. Special warfare is unique in its reliance on indigenous war fighting capacity to stabilize or destabilize operational environments. Special warfare, as a critical capability, and the conceptual application of special warfare in and through cyberspace must address special warfare's contribution to operational art in the human domain. This study uses a qualitative content analysis to explore the linkages between special warfare operations and cyberspace operations to support joint force commanders and U.S. embassy country teams in shaping the human domain. Further, cyber-enabled special warfare is explored through a typology of human action as a framework of analysis to develop methods of integrating cyberspace operations and special warfare.

ACKNOWLEDGMENTS

First and foremost, this thesis was undoubtedly sparked by countless hours of discussion with my good friend Jay K. and his efforts to converge the worlds of cyberspace operations and special warfare. Thank you for your mentorship and candor as I continue to understand your world and leverage its unrecognized strength in executing special warfare on behalf of this great Nation. I am equally indebted to COL Will Bowman, LTC Jerry Moon and my Irregular Warfare Scholars cohort: MAJ Devon Cockrell, MAJ Nic Cruz, MAJ Scott Gilstrap, and MAJ Dan Tucker. Iron truly sharpens iron and I am incredibly grateful for our extremely thought provoking discussions, despite the institutional prisoners' reality in the cave.

Second, I am incredibly thankful and humbled for the personal and professional development that I was able to experience through the candor and guidance provided by my committee. Thank you for your constant support and I look forward to our future collaboration in making Cyber-enabled Special Warfare a reality.

Additionally, I would like to thank COL Patrick Duggan for your candid discussion on your assessment in the development of cyber-enabled special warfare. Your contributions to the body of knowledge have laid large portions of the foundation for my research. Finally, I would like to thank Mrs. Ann Chapman for her diligent efforts in providing the most technical guidance in preparing this thesis for review and approval by the College. Thank you for your patience and technical expertise in the final compilation of work in this thesis.

TABLE OF CONTENTS

Page

ACRONYMS

CE-SW	Cyber-enabled Special Warfare
CEMA	Cyberspace Electromagnetic Activities
DCO	Defensive Cyberspace Operations
DODIN	Department of Defense Information Network
ISR	Intelligence, Surveillance, and Reconnaissance
NDAA	National Defense Authorization Act
OCO	Offensive Cyberspace Operations
OPE	Operational Preparation of the Environment
OSS	Office of Strategic Studies
USASOC	United States Army Special Operations Command
USCYBERCOM	United States Cyber Command
USSOCOM	United States Special Operations Command

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

The merging of military operations and cyberspace operations is growing to meet the adversarial cyber-threats of state and non-state actors and opportunities to counter those threats in and through cyberspace. The United States Special Operations Command (USSOCOM) addresses cyber threats in various ways, largely through special warfare with a focus on the human domain. However, current efforts to integrate special warfare and cyberspace operations fall short of enabling success in the human domain across the whole of government.

The National Defense Authorization Act (NDAA) for fiscal year 2017 has elevated United States Cyber Command (USCYBERCOM) to the status of a unified combatant command. This NDAA brings USCYBERCOM on par with other functional and geographic combatant commands such as USSOCOM and United States Central Command while preventing separation from the National Security Agency.[1] As cyberspace operations are integrated throughout the whole of government, it is important to understand the equities that USCYBERCOM has with the National Security Agency.

USSOCOM has a growing dependence on cyberspace operations to protect forces from adversarial cyber threats and to enhance the execution of special operations. As USSOCOM seeks to integrate cyberspace operations, special operations planners should understand USCYBERCOM's equities while integrating cyberspace operations to support special operations campaigns. The context of the contemporary operational environment provides the conceptual framework for special operations to have strategic

effects through integrating cyberspace capabilities and special warfare by arming special operations teams with asymmetric cyber-tools and irregular warfare tactics[2]

Before discussing USSOCOM's integration of cyberspace operations, it is prudent to differentiate between surgical strike and special warfare. Outside of special operations, the difference may not be readily apparent. Conceptually examining the nature of cyberspace operations and special warfare and their impact on the human domain may enable a greater understanding of how to execute special warfare in and through cyberspace.

The Army Capabilities Integration Center largely conceptualizes multi-domain battle as an extension of combined arms across all domains to outmaneuver adversaries physically and cognitively.[3] This conceptual understanding negates engagement and influence in the human domain in the absence of a combined arms application. This study addresses engagement in the human domain; a holistic and conceptual understanding of the effects that human behavior, security forces, and government have in the operational environment.[4]

Background of the Study

USSOCOM operates across the broad range of military operations where special operations are conducted in support of joint force commands and U.S. embassy country teams. Special operations leadership conceptualized the operational term "gray zone" to address the time and space that exists between steady state security cooperation and anything short of major combat operations.[5] President John F. Kennedy recognized that war in the gray zone was "another type of war, new in its intensity, ancient in its origin—war by guerrillas, subversives, insurgents, assassins . . . seeking victory by

eroding and exhausting the enemy instead of engaging him."[6] Although USSOCOM operates heavily in the gray zone, it is prudent to understand that this zone is a portion of the range of military operations. Successful application of cyberspace in the gray zone may be beneficial across the full spectrum of military operations, to include theater security cooperation under the direction of U.S. embassy country teams.

To gain a better understanding of how to conduct special operations in and through cyberspace, it is necessary to understand the conceptual and operational framework of special operations and cyberspace operations, as well as their historical context. The 2017 NDAA indicates a continued growth of USCYBERCOM as the apparent cyberspace threat from U.S. adversaries has increased. Joint cyberspace doctrine and service component doctrine to support growing cyberspace awareness is continuing to develop; however, this growth does not appear to extend beyond cyberspace-specific doctrine into special operations doctrine. Is there a generational gap in the understanding of emerging capabilities that can be applied in a special warfare environment? Is there a lack of understanding or situational awareness between USSOCOM's special warfare and USCYBERCOM cyberspace operational planners?

For this study, the nature of special warfare in and through cyberspace was examined through a qualitative content analysis and a typology for human action to examine their capacity to enable success in the human domain. The nature of special warfare is protracted and heavily influenced by the human domain, which includes the physical, cultural, psychological, and social environment that affect human behavior of people, security forces, and governments.[7] By examining the current operational approach in conducting cyber-enabled special warfare (CE-SW) in the gray zone,

USSOCOM is in a unique position to enhance current unified campaign plans by operating in and through cyberspace.

Problem Statement

USSOCOM's current incorporation of cyberspace operations falls short of enabling success in the human domain across the range of military operations. There appears to be an operational gap between the training, professional military education, and experience of special warfare personnel to operate in and through cyberspace that inhibits planners in using cyberspace's full capacity. Although cyberspace operations do possess strategic capabilities, purveyors of special warfare should understand the full scope of how to affect the human domain through all layers of cyberspace. Concurrently, there is a dichotomous relationship in the execution between special warfare operations and cyberspace operations. Cyberspace operations planners may also benefit by operating with and through special warfare; however, that extends beyond the scope of this study.

Purpose

The purpose of this qualitative study was to examine USSOCOM's application of special warfare and how cyberspace operations can enable success in the human domain and address the apparent operational gap discussed in the problem statement. The human domain is critical to success in the gray zone, and CE-SW operations should address the need to influence the human terrain in achieving national strategic goals. The qualitative content analysis method was appropriate for this study given the sensitive nature of discussing emerging capabilities and the significance of understanding how special warfare in and through cyberspace affects the human domain.

Significance of the Study

Extensive discussion exists that conceptualizes special warfare and its application within a given operational environment. Emerging cyberspace operations discussion is permeating throughout the Department of Defense. Despite the emphasis of the United States Army Special Operations Command commander in developing cyberspace concepts to support special operations,[8] there are limited discussions that attempt to bridge the dichotomous relationship between special warfare operations and cyberspace operations. Special warfare conducted in and through cyberspace that affects the human domain is the conceptual focus area for this study, examining how special warfare in and through cyberspace can enable success in the human domain across the range of military operations.

Nature of the Study

A qualitative content analysis method was used in this study to facilitate collection, analysis, and interpretation of conceptual application of special warfare operations and cyberspace operations with their effects in the human domain using a typology for human action. A case study methodology would be more appropriate in analyzing the emerging application of cyberspace operations in support of special warfare and its effect in the human domain through the combined training centers and operational employment; however, analysis of capabilities used in those environments exceed the classification of this study. Although the analysis of emerging tactics, techniques, and procedures are not discussed in this study, conceptual analysis through the content analysis method does provide significant latitude to discuss the operational and strategic effects and analyze existing literature regarding CE-SW.

Content analysis research allowed the researcher to analyze written and visual contents to examine the conscious and unconscious beliefs, attitudes, values, and ideas of people and groups.[9] This particular study examined existing literature, independent studies, and doctrine as a source of the content of the analysis. In conducting the content analysis, it allowed the researcher to determine relevant categories to identify and analyze to provide some explanatory power in their specific area of research.[10] The relevant categories in this study sought to address the apparent operational gap regarding USSOCOM's application of cyberspace operations to enable special warfare in the human domain. This study is similar to previous works regarding the linkages between special warfare operations and cyberspace operations and their inherent relationship with the human domain.[11] This study expands on the effects of cyberspace operations to enable special warfare by analyzing their effects in the human domain through a typology for human action.

Research Question

1. Is the current application of operational art suitable for executing special warfare in and through cyberspace?

2. How can/should cyberspace operations be employed to support special warfare in and through cyberspace?

3. How can cyberspace operations strengthen special warfare in influencing the human domain?

Assumptions

Outside of major combat operations, special operations personnel are increasingly deployed to support geographic combatant command theater campaign plans that aim to shape strategic, operational environments. These short duration deployments are part of theater security cooperation programs that are normally executed by special operations personnel at the request of the U.S. ambassador, also known as the chief of mission. These activities support the country team's application of the military instrument of national power and are coordinated through the respective Department of Defense element under the direction of the Senior Defense Official or defense attaché.[12]

The national cyber mission force is a strategic element of the military instrument of national power, and the cyber combat mission force is experiencing a difficult time in talent management of available forces.[13] Although the development of the cyber mission force falls outside the scope of this study, it is important to note the fluid nature of USCYBERCOM's growing force structure to meet the needs of both national requirements as well as the requirements of unified combatant commanders. The above-stated difficulty in personnel management is also addressed in the literature review of cyberspace operations in chapter 2 and perceived to be an assumption of the continued development of USCYBERCOM.

Definitions and Descriptions

The prudent use of key terms throughout this study is deliberate and necessary in delineating between terms often used interchangeably within the special operations and cyberspace operations communities. Select terms are discussed below to provide a common understanding and to promote clarity in addressing this study. Given the

military nature of this study, doctrine provides a common understanding within the context of this qualitative content analysis study.

Cyber-Enabled Special Warfare. CE-SW is not used in special warfare doctrine, but has been coined by other academic writing.[14] This study defines CE-SW as a complementary special warfare capability providing the means to compliment the effects of foreign internal defense/unconventional warfare/counterinsurgency through unique approaches in and through cyberspace. Although CE-SW is a complementary capability within a special warfare campaign, capabilities are and must remain directly nested through existing delegated authorities with other government agencies. CE-SW is produced through the combination of special warfare requirements, desired effects, and the collaboration of information concerning activity in cyberspace and the electromagnetic spectrum. Unlike cyber operations, CE-SW is special warfare-centric based on influencing the human domain within cyberspace.[15]

Cyberspace Operations. Cyberspace operations, from a joint perspective, are broadly described as the employment of cyberspace capabilities in and through cyberspace to support military, intelligence, and ordinary business operations of the Department of Defense.[16] The use of the term cyberspace operations in this qualitative study refers to the military component of cyberspace operations that are aimed at achieving joint force commander military and U.S. country team objectives. Department of Defense Information Network (DODIN) operations are not discussed given they are inherent to the ordinary business operations component. In general, cyberspace operations affect access while the military uses cyberspace to conduct military operations to influence and shape the information environment.

Cyberspace. According to Joint Publication (JP) 3-12 (R), *Cyberspace Operations* is one of five interdependent domains that include air, land, maritime, and space. Cyberspace is a global domain within the information environment that relies on an interdependent network of information technology infrastructures of links and nodes that reside in the physical domain.[17] See chapter 2 for a more comprehensive discussion regarding the layers of cyberspace that include the physical network, logical network, and cyber-persona layers. Given the nature of cyberspace, there is significant overlap of operations the joint force commander may employ that may enable or inhibit operations in and through cyberspace. These domain overlaps include but are not limited to electronic warfare; electromagnetic spectrum management; command and control systems; intelligence, surveillance, and reconnaissance (ISR); navigation warfare; and some space missions.[18]

Defensive Cyberspace Operations (DCO). The joint definition for DCO is "passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities to protect data, networks, net-centric capabilities, and other designated systems."[19] Again, it is important to note the characterization of cyberspace operations are categorized by intent and additional discussion in chapter 2 highlights cyberspace actions that contribute to DCO.

Human Domain. Special operations leadership emphasizes the engagement function concept that provides a foundation that underpins the human domain.[20] USSOCOM defines the human domain as "the people (individual, groups, and populations) in the environment, including their perceptions, decision-making, and behavior."[21] The human domain is characterized by a need to understand the social,

cultural, physical, informational, and psychological elements that shape this domain.[22] United States Army Training and Doctrine Command also addresses engagement as a functional concept and defines the human domain as "the totality of the physical, cultural, psychological, and social environments that influence human behavior," emphasizing designed applications that "influence, fight, and win in population-centric conflicts."[23] This study uses the USSOCOM definition as the domain being the people that are primed and/or queued through the characterization underlying social, cultural, physical, informational, and psychological elements. In an environment where the fight is for the middle ground, understanding the human domain provides insight into populations that are primed and queued for action based on the operational environment. Chapter 2 expands on the effects of special warfare in the human domain and the contribution to the operational environment.

Offensive Cyberspace Operations (OCO). The joint definition used for OCO is "cyberspace operations intended to project power by the application of force in or through cyberspace."[24] Although a significant amount of military business takes place in cyberspace, OCO specifically refers to the intended projection of power. JP 3-12(R) also addresses cyberspace actions that may fall into OCO; however, it is important to note that military missions in cyberspace are categorized by intent that may not be readily apparent based on the cyberspace action being performed.[25] Chapter 2 provides a more in-depth discussion of the nature of OCO and what cyberspace actions contribute to OCO.

Operational Art. The joint definition of operational art is "the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ

military forces by integrating ends, ways, means."[26] Where the joint operations planning process is more iterative and structured, operational art is the deliberate metacognitive awareness process that a joint force commander balances the art of command versus the science of control.

Special Operations. In this study, the term special operations refers to operations that require "unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments."[27] The nature of special operations is usually characterized by one or more of the following criteria: "time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk."[28] It is important to note that special operations encompass all the separate military branch contributions to special operations. The term special operations in this study is from the joint military perspective that includes the contributions of each military branch to execute special operations.

Special Warfare. Special warfare is one of the two critical capabilities of Army Special Operations' contributions to unified land operations to support a joint force commander. Special warfare includes lethal and nonlethal operations taken by Army special operations forces that have a deep understanding of culture and foreign language, small unit tactics, and are capable of operating alongside indigenous forces in permissive, uncertain, or hostile environments.[29] It is important to note that special warfare can be conducted independently of or in conjunction with conventional operations. Special warfare is commonly understood to take place in the gray zone; however, special warfare operations do span the entire range of military operations from theater security

cooperation under the direction of a U.S. embassy country team or under the command of a joint force commander in a declared combat zone.

Surgical Strike. Surgical strike is the second critical capability of the Army special operations' contribution to unified land operations in achieving a joint force commander's strategic goals. Surgical strike is the execution of activities that employ special operations to seize, destroy, capture, exploit, recover, or damage designated targets or influence threats within an area of operations.[30] Surgical strike operations, similar to special warfare, are also conducted in hostile, denied, or politically sensitive environments.[31] Although this study focuses on the application of special warfare, specific surgical strikes are conducted in a special warfare environment that affects the layers of cyberspace and the human domain.

Limitations

The author maintains access to personnel within USSOCOM and USCYBERCOM that are undergoing efforts to develop an operational approach to conducting special operations in and through cyberspace. However, due to the nature of ongoing development of cyberspace operations in support of special operations and the sensitivity of capabilities, this study will not specifically discuss cyberspace operations or cyberspace capabilities employed in the contemporary operational or training environments. Several training concepts and events have incorporated CE-SW; however, the discussion and research of said events fall outside the scope of this study and are areas for further research at the appropriate classification level.[32]

Scope and Delimitations

This study used a content analysis to explore the feasibility and suitability of a social science typology model to enable special warfare operations in and through cyberspace. Through an operational approach to supporting country team and geographic combatant command theater security cooperation programs, this research explored special operations employment under various titles of U.S. Code and defense authorizations. Through the contemporary employment of special operations, explored implications of CE-SW and determined whether the proposed links between special operations and cyberspace operations are mutually beneficial to USSOCOM and USCYBERCOM. Further, the study assessed if these operational links contribute to the U.S. strategic comparative advantage through the current approach to operational art.

Summary

Chapter 1 introduced the concept of cyberspace operations being employed to support special warfare in the human domain. CE-SW is a strategic capability gap[33] that this study examines through a qualitative content analysis research study to examine CE-SW through a typology of human action. The results of this study attempt to provide a lens of examining underpinnings of the human domain that can be directly targeted through cyber-enabled special operations. Chapter 2 explores the historical context and contemporary use of special warfare and the dichotomy between special warfare operations and cyberspace operations. It highlights existing discussions on cyberspace operations employed to support special warfare in and through cyberspace, the application of operational art in special warfare, and how cyberspace operations may enable special warfare to succeed in the human domain.

[1] U.S. Congress, House, Report 118-840, *National Defense Authorization Act for Fiscal Year 2017* (NDAA), Conference Report to Accompany HR S. 2943 (Washington, DC: November 30, 2016), accessed July 30, 2017, https://www.congress.gov/congressional-report/114th-congress/house-report/840/1; 360; Mark Pomerleau, "Congress Set to Elevate CYBERCOM to Unified Combatant Command," C4ISRNET, December 2, 2016, accessed June 6, 2017, http://www.c4isrnet.com/articles/congress-authorizes-elevating-cybercom-to-unified-combatant-command. This assertion assumes the U.S. President approves the NDAA. As of the publication of this study, the NDAA does not have presidential approval.

[2] GEN Joseph L. Votel, USA, Commander, U.S. Central Command, email correspondence with COL Patrick Duggan, December 18, 2014, quoted in Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Forces Quarterly*, no. 79 (4th Quarter 2015): 46, accessed June 6, 2017, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/Article/621123/strategic-development-of-special-warfare-in-cyberspace/.

[3] Army Capabilities Integration Center, *Multi -Domain Battle: Combined Arms for the 21st Century*, U.S. Army, accessed June 6, 2017, http://www.arcic.army.mil/App_Documents/Multi_Domain_Battle.pdf, 1.

[4] LTG (RET) Charles T. Cleveland, MG James B. Linder, and WO3 Ronald Dempsey, "Special Operations Doctrine: Is it Needed?" *PRISM: Special Operations in a Chaotic World* 6, no. 3 (2016): 17.

[5] Ibid., 7, 15; CAPT Philip Kapusta, "The Gray Zone," *Special Warfare* 28, no. 4 (October 2015): 18-25, accessed June 6, 2017, http://www.soc.mil/SWCS/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf; GEN Joseph L. Votel, LTG(RET) Charles T. Cleveland, COL Charles T. Connet, and LTC(RET) Will Irwin, "Unconventional Warfare in the Gray Zone," *Joint Forces Quarterly*, no. 80 (1st Quarter 2016): 101-109, accessed June 6, 2017, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

[6] The American Presidency Project, "President John F. Kennedy Remarks at West Point to the Graduating Class of the U.S. Military Academy, West Point, NY, June 6, 1962," accessed July 30, 2017, http://www.presidency.ucsb.edu/ws/?pid=8695.

[7] Department of the Army, Headquarters U.S. Army Training and Doctrine Command (HQ TRADOC), TRADOC Pamphlet (PAM) 525-8-5, *The U.S. Army Functional Concept for Engagement* (Washington, DC: Fort Eustis, VA, 2014), 36; Cleveland, Linder, and Dempsey, 17.

[8] Headquarters, Department of the Army (HQDA), Army Doctrine Publication (ADP) 3-05, *Special Operations* (Washington, DC: Government Printing Office, 2012), forward.

[9] Norman E. Wallen and Jack R Fraenkel, *Educational Research: A Guide to the Process* (Mahwah, NJ: Taylor & Francis[CAM], 2001), accessed April 16, 2017c EBSCOhost, 408.

[10] Ibid.

[11] Duggan, "Strategic Development of Special Warfare in Cyberspace," 46-53; Patrick M. Duggan, "Man, Computer, and Special Warfare," *Small Wars Journal* (January 4, 2016), accessed June 6, 2017, http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

[12] Joint Chiefs of Staff (JCS), Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: Department of Defense, 2014), III-13.

[13] COL Kevin P. Romano, "Army Cyber Mission Force: Ambitions and Realities" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2015), 37-38.

[14] Duggan, "Strategic Development of Special Warfare in Cyberspace," 52.

[15] The development of this definition was modeled using the conceptualization of cyber-enabled intelligence as referenced in Headquarters, Department of the Army, Army Doctrine Reference Publication 2-0, *Intelligence* (Washington, DC: Government Printing Office, 2012), 48-49.

[16] Ibid.

[17] Joint Chiefs of Staff (JCS), Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: Department of Defense, 2013), I-2.

[18] Ibid., II-1.

[19] Ibid., 69.

[20] Cleveland, Linder, and Dempsey, 17.

[21] U.S. Special Operations Command, *Operating in the Human Domain* (McDill Air Force Base, FL: Headquarters, U.S. Special Operations Command, 2015), 76.

[22] Ibid.

[23] HQ TRADOC, TRADOC PAM 525-8-5, 36.

[24] JCS, JP 3-12, 69.

[25] Ibid., 25.

[26] Joint Chiefs of Staff, Joint Publication 5-0, *Joint Operational Planning* (Washington, DC: Department of Defense, 2011), 257.

[27] JCS, JP 3-05, GL-11.

[28] Ibid.

[29] HQDA, ADP 3-05, 9.

[30] Ibid.

[31] Ibid.

[32] For further information regarding the observations of contemporary integration of CE-SW, contact the Center for Army Lessons Learned and the USASOC Lessons Learned.

[33] Duggan, “Strategic Development of Special Warfare in Cyberspace,” 52.

CHAPTER 2

LITERATURE REVIEW

Introduction

There is an increase of special operations and cyberspace operations use in the contemporary operational environment to address the growing state and non-state threats to the U.S. strategic national interest. Despite the operational employment of special warfare and cyberspace operations, USSOCOM may stand to benefit from examining the effects of CE-SW and how to leverage those tools to create asymmetry. Iran and Russia have successfully demonstrated how to leverage CE-SW to create asymmetry. Despite Russia's and Iran's success, a strategic level capability gap for the U.S. military to integrate CE-SW remains.[1]

Surgical strike and special warfare are special operations that are critical in shaping the operational environment, preventing conflict, and winning the nation's wars that require the inherent and integrated use of cyberspace operations.[2] The nature of the conflict in the contemporary operational environment has demonstrated the increasing need to develop better methods to address the complexity of engagements within the human domain.[3] When integrating cyberspace operations to enable special operations, it is necessary to understand the nature of special operations and what special warfare's contribution to operational art is in achieving national strategic objectives. How do special warfare operations in and through cyberspace contribute to special warfare's contribution to operational art?

Chapter 2 contains a discussion of historical and contemporary literature regarding special warfare and cyberspace operations as they pertain to enabling special

warfare in and through cyberspace. It further examines the focus on special warfare's contribution to operational art and explores the linkages between special warfare, cyberspace operations, and the human domain.

Special Warfare and Surgical Strike

Special operations' contributions to dominate the land domain are surgical strike and special warfare. These two mutually supporting forms of special operations encompass the American way of special operations warfighting that supports the Army's operating concept in shaping the operational environment, preventing conflict, and winning the nation's wars.[4] The most comprehensive discussion of the delineation between surgical strike and special warfare is Army Doctrine Publication (ADP) 3-05, *Special Operations*. The primary distinction is that surgical strike operations are primarily short duration unilateral operations[5] and special warfare operations are mostly long duration and targeted at training, advising, and assisting indigenous forces in conducting special operations and building indigenous war fighting capacity.[6]

There is a growing reliance on the indigenous war fighting side of special warfare to decrease the reliance on deploying large numbers of U.S. conventional soldiers.[7] In the classic sense of Carl von Clausewitz's paradoxical trinity (force, reason, and chance), the execution of special warfare highlights the complex nature of war being more complicated than a chameleon that adapts is characteristics to a particular environment.[8] If the will of the people does not support a growing commitment of a vast number of conventional forces, the administration is compelled to develop policy that addresses the contemporary nature of war. While a more in-depth study could highlight the various nature of war within a special warfare context concerning Clausewitz's trinity, it is

important to note the acknowledgment of Clausewitz's assertion as to the fluid nature of war and the development of special warfare operations in the contemporary operational environment. The use of cyberspace within the contemporary operational environment amplifies ambiguity, and it increases the fog and friction of war. Special operations can be conducted without conventional operations; however, the proper blending of special operations and conventional military operations may increase the effectiveness of shaping activities and improve execution of counterterrorism and irregular warfare.[9]

Overall, surgical strike and special warfare are the Army's special operations contribution to unified land operations, but special warfare is inherently intertwined with aspects of the human domain. Joint force commanders should understand the strategic advantages of employing special warfare: improved understanding and shaping of the environment, cost-imposing strategies, managed escalation and credibility risk, and sustainable solutions.[10] It is important to note that outcomes of surgical strike operations do affect the human domain; however, special warfare operations have a reliance on the human domain for success throughout a special warfare campaign with a heavy dependence on indigenous war fighting capability.

A History of U.S. Special Warfare

Authors such as Robert Asprey and Max Boot provide a significant body of work on historical guerrilla warfare and small war campaigns from the U.S. revolution through the contemporary operating environment. It is important to note that focus of this study is the concept of U.S. sponsored special warfare operations that emerged during World War II to the present.[11] This emphasis is on special warfare operations that are reliant on the ability of indigenous war fighting capacity. The origins of modern special warfare

operations are seeded in President Franklin D. Roosevelt's creation of the Coordinator of Information, which later became the Office of Strategic Services (OSS) during World War II.[12] The members of the OSS were learning unique aspects of unconventional warfare that were as old as history itself, which were employed by Hannibal Barca and Alexander the Great in their unconventional guerrilla campaigns.[13]

One of the notable OSS contributions to special warfare was the use of unconventional warfare in the European and Pacific theaters. Jedburgh Teams, named after the Jedburgh area of Scotland where the local Scots conducted guerrilla warfare in the twelfth century against the British, were parachuted behind enemy lines and coordinated French Maquis activities in support of the Allied liberation of France.[14] Detachment 101 successfully worked with and through the Kachin tribesmen in conducting unconventional warfare to support conventional operations against the Japanese in Burma.[15] These early uses of special warfare acted as a force multiplier to train and organize larger groups of guerrilla fighters in Nazi-occupied France and Burma; however, despite the development of these special operations units, the OSS was disbanded following significant post-war cuts with no residual peacetime special operations capacity.[16]

In the wake of Soviet support to wars of national liberation, President Kennedy pushed for the development of counterinsurgency doctrine to address this growing strategic threat. Portions of the new counterinsurgency doctrine were taken from Colonel Russell Volckmann's lessons learned from working with partisans in World War II.[17] In 1962, the Overseas Internal Defense Policy established indigenous responsibility for defeating insurgencies and set the conditions for contemporary partner capacity

development, emphasizing the need for unity of effort across the whole of government.[18] The precedent established during the development of special warfare under President Kennedy has shaped the current application of foreign internal defense during phase zero to support both joint force commanders and U.S. embassy country teams. See discussion under special warfare's contribution to operational art for a contemporary conceptual model of special warfare that incorporates foreign internal defense, unconventional warfare, and counterinsurgency.

Operational Art

As the military prepares to execute operations in support of a joint force commander or theater security cooperation under a U.S. embassy country team, it is critical for the commander and his staff to understand the need for a conceptual approach in tandem with traditional planning processes that tend to be more methodical and regimented. The Joint Chiefs of Staff designate this conceptual approach as operational art: "the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, means."[19] In the contemporary operating environment, strategy is increasingly being developed to address non-state threats, where convenient Clauswitzian centers of gravity are not well defined, and Jominian lines of operations may be ambiguous in identifying decisive points in dealing with non-state threats.[20]

Harry Yarger expounds upon ends, ways, and means within the context of the instruments of national power. The instruments of national power are commonly referenced to as diplomatic, information, military, and economic and it is prudent that

military planners understand the importance of developing and maintaining unity of effort across the instruments of national power when conducting campaign design. Yarger asserts that "objectives (*ends)* explain 'what' is to be accomplished . . . strategic concepts (*ways)* explain 'how' the objectives are to be accomplished by the employment of the instruments of national power," and "resources (*means*) in strategy formulation determine the types and levels of resources that are necessary to support the concepts of strategy."[21] In developing strategic ends, ways, and means, it is important to understand the operational environment and the contextual applications of resources and their second/third order effects to meet a strategic end state. As the U.S. military continues integration of cyberspace operations and military operations in and through cyberspace, understanding intelligence gain/loss and the potential for the compromise of intelligence activities is a concern that should be assessed.[22]

When developing strategy and applying operational art, understanding the operational environment is fundamental in identifying how the human domain may be primed and queued for human action to support either an incumbent or insurgent. Clausewitz considered war by popular uprising to be a phenomenon of the nineteenth century,[23] but is it a phenomenon of the nineteenth century or is there a cognitive dissonance that causes incumbent governments to discount irregular warfare and insurgents such as Mao Zedong to embrace it? Regardless, the success of the Chinese communists in 1949 associated with Mao's writing of *On Guerrilla Warfare*, the diffusion of European empires in Asia and Africa, and the Cold War contribute to the salience of contemporary application of revolutionary warfare: "what is new is not the phenomenon itself, but our perception of it."[24] In the contemporary operational

environment, purveyors of special warfare should be in tune with the human domain's effect on the success of applying operational art.

The USASOC states the first special operations forces imperative is to "understand the operational environment."[25] The intuitive paradigm in this statement suggests the implicit cognition of the fluid nature of special operations and special warfare strategic approaches and the environments that they are employed. The application of special operations in support of theater security cooperation and U.S. embassy country teams has also seen a shift due to four contributing factors: "a national strategic emphasis on partner engagement and multilateralism, a globally oriented and organizationally maturing SOCOM, the proliferation of non-state threats less susceptible to conventional warfare, and the global diffusion of power."[26] Varying thoughts contribute to the catalyst of the diffusion of power. Some of these catalysts include the nuclear age and the impracticality or dangerous nature of war between great military powers to great powers being ponderously prepared for big war and thus vulnerable to tactics of revolutionary war.[27] Acknowledging the current context and use of special warfare, vice the causal relationship of what forced this shift in contemporary strategy, there is significant cause to explore special operations contribution to operational art.

Special Warfare's Contribution to Operational Art

Special warfare differs from the application of conventional military operations in that sustained engagement is a crucial contribution to special warfare. Through sustained engagement, special warfare operational art logically helps joint force commanders in connecting tactics to strategy through situational understanding, influence, and capacity building. The implication is that "special warfare's unique contribution to operational art

consists of the mobilization of partners strategic and operational centers of gravity, and the neutralization or integration of the enemy's, in the human domain."[28] This mobilization may take place by bolstering institutional training and equipping of partner forces or by queuing segments of the population that may be primed for human action. Human action may range from participation in military operations or just taking part in the proliferation of non-violent action to achieve political ends, popularized buy books such as *From Dictatorship to Democracy: A Conceptual Framework for Liberation* by Glenn Sharpe.[29]

Figure 1, developed by the RAND Corporation, provides a graphic depiction of the contrast between unilateral U.S. military operations and special warfare campaigns where local partners are the main effort. Special warfare is further divided based on either desired stabilizing effects or destabilizing effects. Based on this graphic depiction in contemporary military doctrine, foreign internal defense is a special warfare campaign executed with and through local partners to stabilize a given operational environment. In contrast, unconventional warfare is a special warfare campaign implemented with and through local partners to destabilize a given operational environment.

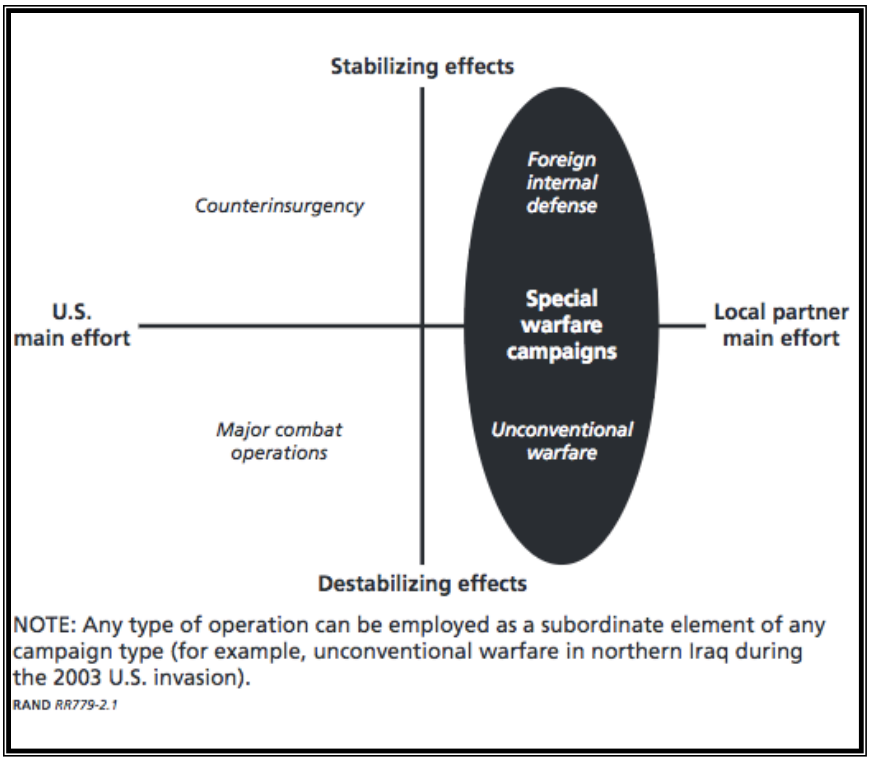

Figure 1. Local Partners and Special Warfare Campaigns

Source: Dan Madden, Dick Hoffman, Michael Johnson, Fred T. Krawchuk, Bruce R. Nardulli, John E. Peters, Linda Robinson, and Abby Doll, *Toward Operational Art in Special Warfare* (Santa Monica, CA: Rand Corporation, 2016), 41.

Understanding special warfare's unique contribution to operational art in the human domain, military operations conducted in support of a special warfare campaign should address effects in the human domain. All military operations, to an extent, have effects in human domain. However, special warfare's inherent reliance on indigenous partner capacity provides commanders with unique situational awareness where special operations forces must influence partners, enemies, and the people throughout the operational environment. As the proliferation of technology increases the complexity of

the information environment, special warfare campaigns have unique access to cyberspace through placement of forces and relationships with local partners.

Special Warfare and the Human Domain

Overall, the continuum of warfare has varying degrees of effects within the human domain. What is important to note is that special warfare relies heavily on indigenous capacity, where the use of conventional forces while conducting unilateral operations is not as reliant on an indigenous capacity. Some anecdotal examples of a more traditional understanding of attempting to influence the human domain include Alexander the Great's concept of *Homonoia*, or Hannibal's success in "[propitiating] the native tribes."[30] Another anecdotal example during a British special warfare campaign was the influence T. E. Lawrence provided through his engagement with Arab tribes during World War I.[31] These examples, although anecdotal, do highlight the historical significance in understanding the importance that engagement has shaped and influenced conventional military campaigns, implying the value of the U.S. Army and USSOCOM's operational concept of engagement.

The above special warfare continuum highlights the reliance on local partners to achieve the strategic end state where engagement plays a more prominent role. Within the context of engagement, it is important to note that special warfare shapes indigenous capacity through engagement while simultaneously influencing a population's perspective of the incumbent or the insurgent. An example of U.S. special operations' engagement provides additional insight below on how engagement has helped shape the human domain within the context of special warfare.

Dixie Bartholomew-Feis discusses the factors that contributed to the OSS collaborating with the Viet Minh in the Indochina region during World War II, asserting OSS's understanding of the "human factor."[32] This concept of the human factor underlines the importance of engagement and the acknowledgment of influencing the human domain. Allison Thomas, an OSS Deer Team leader, was disappointed to find his aide-de-camp had passed away when he visited Vietnam years later, but the fond recollections of their relationships had been passed down through generations, and he was pleased to find a photo of the Deer Team in the living room of his aide-de-camp.[33] The human factor and the relationships built with the Viet Minh are further illustrated in one of the last meetings between then President Ho Chi Minh and OSS member Major Frank White.

Being surrounded by Chinese, British, and French colonels and generals as well as members of Ho's cabinet, Major White hoped to slip out after everyone had taken their seats only to find the seat next to President Ho Chi Minh reserved for the former OSS member.[34] Considering the strategic context of this last meeting of an OSS member, it may be more anecdotal, but the nature of their relationship provides some insight into the significance of special operations engagement. Although the strategic environment prevented the United States from nurturing this relationship as France sought to re-exert their influence in Indochina, this is one example of how special warfare applies engagement to influence partner forces and at the time build capacity to meet U.S. strategic objectives.

Cyberspace Operations

Joint operations increasingly rely on the integrated use of cyberspace, a global domain that lies within the information environment and made up of multiple layers. Of note, the information environment is "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information," and are broken down into physical, informational, and cognitive dimensions.[35] As the use of cyberspace proliferates, the U.S. military, as well as allies and other partners, stand to gain and maintain strategic advantages in the operational environment by exploiting developments in cyberspace capabilities.[36] First, it is prudent for cyberspace operations planners to thoroughly understand cyberspace as a domain and the layers that comprise cyberspace.

Cyberspace consists of overlapping networks, nodes, and system data that are increasingly interconnected, but sometimes isolated to control access. Cyberspace is doctrinally described regarding three layers where cyberspace operations maybe conducted: physical network, logical network, and cyber persona layers.[37] These three layers provide the conceptual framework to understand how cyberspace logically interacts with the operational environment. Understanding the natural interaction of cyberspace layers is critical to understanding how activities in cyberspace affect the physical domains. Also, activities in the physical domain can create effects in and through cyberspace by manipulating the electromagnetic spectrum or the physical infrastructure that supports cyberspace.[38]

The first layer of cyberspace is the physical network layer with two main components consisting of geographic location and physical device. These are represented in hardware, system software, and infrastructure that support the network and physical

connectors.[39] The physical network layer of cyberspace can be targeted through direct physical means of the physical components or the electromagnetic spectrum. The electromagnetic spectrum is a wireless transfer medium for links in cyberspace operating on a range of frequencies of electromagnetic radiation from zero to infinity. Cyberspace's increased reliance on wireless capabilities can be targeted through electromagnetic spectrum operations.[40] Chapter 4 discusses this in more detail regarding special operations teams-alpha and organic special operations capacity that contribute to intelligence operations.

The second layer of cyberspace is the logical network that consists of "elements of the network that are related to one another in a way that is abstracted in the physical network."[41] Some simple examples of this are any websites posted on multiple servers in different locations accessible by a single uniform resource locater or compiled lines of code that process the flow of data in and through cyberspace.[42] A conventional method to target the logical network layer of cyberspace is malware. The third cyberspace layer, the cyber persona layer, represents a higher level of abstraction of the logical network where cyber personas may relate to actual people or entities. In some cases, one user may have multiple personas, and some personas may have multiple users. This layer of cyberspace creates a degree of complexity and ambiguity where attributing responsibility and targeting in cyberspace is difficult for creating a joint force commander's desired effect.[43]

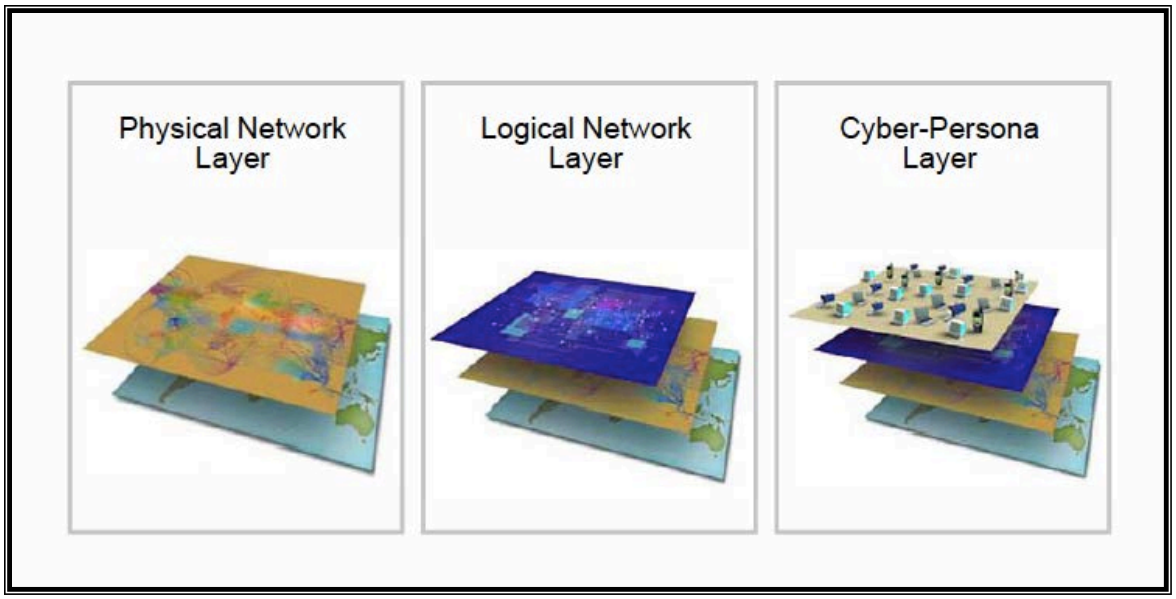

Figure 2. The Three Layers of Cyberspace

Source: Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: Department of Defense, 2013), fig. I-1.

Cyberspace operations employee capabilities in cyberspace where the primary purpose is to achieve objectives in cyberspace. The effects of cyberspace operations overlap with the space and physical domains that may enhance the operational effectiveness of electronic warfare, electromagnetic spectrum management, command-and-control, and ISR.[44] Cyberspace operations include OCO, DCO, and DODIN operations that are categorized based on their intent and underpinned by adequate operational preparation of the environment (OPE).[45] Cyberspace forces execute cyberspace actions that include cyberspace defense, cyberspace ISR, cyberspace OPE, cyberspace attack, and cyberspace security.[46] Although DODIN is vital to everyday military operations, OCO, and DCO are the primary focus of this study.

Empirical studies regarding the development of the cyber mission force emphasize the need to recruit, retain, and organize cyber forces to meet the demand of the U.S. Army. Current strategies indicate difficulty with recruitment and retention, while also fostering an environment where technical skills outweigh the need to develop operational leaders. In addition to the talent management, the Army has disbursed cyberspace capabilities across the Signal Corps, the Military Intelligence Corps, and the cyber career field 17.[47] If this empirical study holds, it will take time for cyberspace forces to fill the Army cyber mission force and to project capacity to conduct cyberspace operations across the Army. As the development of the cyber mission force is a capability gap, does USSOCOM have the ability to develop organic capacity to conduct special operations in and through cyberspace?

Special Warfare through Cyberspace

The increasing capacity for joint force commanders to conduct cyber electromagnetic activities should meet and contribute to strategic objectives. As the Army seeks to expand cyberspace operations training and education, operational and strategic planners will develop the necessary experience to integrate CEMA (cyberspace electromagnetic activities) more seamlessly into operations. In doing so, former Commander of USCYBERCOM, Admiral Michael Rogers, highlights the need to build partnerships and develop structures and processes that generate options to narrow the gaps between the stakeholders that rely on the use of cyberspace.[48] Within the joint environment, the joint operational planning process provides the systematic process to integrate cyber electromagnetic activities to support operations.[49]

Within special operations, there seems to be an institutional lack of training, education, and experience to employ cyberspace operations at the tactical, operational, and strategic levels.[50] This perceived gap inhibits leaders across USSOCOM from enabling special warfare in leveraging cyberspace. From a training perspective, the United States Army Training and Doctrine Command is addressing this to some degree with developing centers of excellence and incorporating various branch representatives within the respective centers.[51] Although, there is an apparent gap in the doctrine that indirectly shapes professional military education of special operations leadership. This apparent gap prevents understanding how to conduct cyber-enabled special operations and leverage cyberspace to influence the human domain.

Colonel Patrick Duggan asserts that "cyber-warfare is human warfare" and that the use of cyberspace is the latest change in the form of warfare which is an inherently a human enterprise.[52] Iran's response to the Green Movement, assistance to the Syrian regime, and Russian actions in the Ukraine has demonstrated four things. One, there is a distinction between tactical and strategic level cyberspace capabilities. Two, CE-SW is a proxy-executed endeavor that capitalizes on the limited attribution of the cyber persona layer of cyberspace. Three, cyberspace actions and information operations play a significant role in cyber-enabled irregular warfare. Four, CE-SW could both deter conflict and be used across the range of military operations.[53]

If the contribution of special warfare to operational art is heavily reliant on the human terrain and cyber-warfare is an extension of human warfare, then a social framework for influencing the human domain may provide insight into how special warfare in and through cyberspace can enhance special warfare's contribution to

operational art. When understood through the paradigm of special warfare, all three layers of cyberspace involve a significant degree of human interaction, which creates interdependence between each layer. This relationship fosters an environment where multiple modes and methods can be applied directly or indirectly to influence the human domain through the layers of cyberspace.

Gap in Literature Leading to the Study

Cyberspace operations doctrine and the cyber defense strategy are relatively new within the joint operating environment. Although retired Lieutenant General Charles Cleveland stated the need for inherent and integrated cyberspace operations in the forward of ADP 3-05, it is important to note that cyberspace operations are not mentioned through the entirety of the body of the doctrine publication. Cyberspace operations from the joint perspective were in the nascent stages of doctrine development in 2012, with JP 3-12 (R) being published in 2013. Similarly, the Army, under the direction of President Kennedy, developed counterinsurgency doctrine through the J.F.K. Special Warfare Center and School in early 1960 but failed to incorporate it throughout the contemporary doctrine at the time for mass consumption of all Army specialties.[54] The Army writ large rediscovered the need for counterinsurgency in 2003 following the liberation of Iraq, and collectively shifted focus to create doctrine, while extensive work had been done previously.

Some parallels exist with the current development of cyberspace operations doctrine, as cyberspace operations are slowly matriculating into operational doctrine for the remaining army branches. CE-SW has been coined by contemporary literature discussing the application of special warfare in and through cyberspace, however, despite

the growing dependence on the use of cyberspace little has been introduced into the current contemporary special operations doctrine. USSOCOM is in a position to enable success in the human domain by closing the gap in CE-SW.

Summary

Chapter 2 discusses the contemporary literature that addresses the linkages between special warfare, cyberspace operations, and the application across the range of military operations to influence the human domain. Given the inherent reliance of special operations on the human domain, CE-SW should leverage its effects to influence human behavior as well as traditional cyberspace operations effects to provide or limit access and freedom of maneuver to adversaries in cyberspace. In an environment where special warfare is aimed at stabilization or destabilization of an adversary in an operational environment, special warfare in and through cyberspace provides unique operational frameworks to influence the human domain that must be understood from a context of human action.

---

[1] Duggan, "Strategic Development of Special Warfare in Cyberspace," 47, 52.

[2] HQDA, ADP 3-05, forward.

[3] Dan Madden et al., *Toward Operational Art in Special Warfare* (Santa Monica, CA: Rand Corporation, 2016), xiv.

[4] HQDA, ADP 3-05, forward.

[5] Ibid., 8.

[6] Ibid.; Madden et al., 21.

[7] Cleveland, Linder, and Dempsey, 10.

[8] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Oxford, England: Oxford University Press, 2007), 61.

[9] HQDA, ADP 3-05, 16.

[10] Madden et al., xv.

[11] Robert B. Asprey, *War in the Shadows: The Guerrilla in History,* vol. 1 (Lincoln, NE: IUniverse, 2002; Robert B. Asprey, *War in the Shadows: The Guerrilla in History*, vol. 2 (Lincoln, NE: IUniverse, 2002); Max Boot, *The Savage Wars of Peace: Small Wars and the Rise of American Power* (New York: Basic Books, 2014).

[12] Alfred H. Paddock Jr., *Special Warfare: It's Origins* (Lawrence: University Press of Kansas, 2002), 151.

[13] MG (RET) John K. Singlaub, in Dwight John Zimmerman and John D. Gresham, *Beyond Hell and Back: How America's Special Operations Forces Became the World's Greatest Fighting Unit* (New York: St. Martins Griffin, 2008), 9; Asprey, vol. 1, 6-9.

[14] Paddock, 28; COL Aaron Bank, *From OSS to Green Berets: The Birth of Special Forces* (New York: Simon and Schuster, 1986), 25, 74.

[15] Paddock, 27.

[16] Ibid., 31; Zimmerman and Gresham, 15.

[17] Andrew J. Birtle, *U.S. Army Counterinsurgency and Contingency Operations Doctrine 1942-1976* (Washington, DC: Center for Military History U.S. Army, 2006), 230-238.

[18] Overseas Internal Defense Policy, attached to National Security Action Memorandum 182, Counterinsurgency Doctrine, September 1, 1962, in Andrew J. Birtle, *U.S. Army Counterinsurgency and Contingency Operations Doctrine 1942-1976* (Washington, DC: Center for Military History U.S. Army, 2006), 238-239.

[19] JCS, JP 5-0, 257.

[20] Clausewitz, 242; John Shy, "Clausewitz," in Peter Paret, Gordon Alexander Craig, and Felix Gilbert, *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, NJ: Princeton University Press, 1986), 144.

[21] Harry R. Yarger, *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2006), 52-62.

[22] JCS, JP 3-12, 30.

[23] Clausewitz, 184.

[24] John Shy and Thomas W. Collier, "Revolutionary Warfare," in Peter Paret, Gordon Alexander Craig, and Felix Gilbert, *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, NJ: Princeton University Press, 1986), 838.

[25] U.S. Special Operations Command, "SOF Imperatives," U.S. Army, 2017, accessed March 28, 2017, http://www.soc.mil/USASOCHQ/SOFImperatives.html.

[26] Brian S. Petit, *Going Big by Getting Small: The Application of Operational Art by Special Operations in Phase Zero* (Denver, CO: Outskirts Press, 2013); Joseph S. Nye, Jr., *The Future of* Power, (New York: Public Affairs, 2011).

[27] Shy and Collier, 818.

[28] Madden et al., 65.

[29] Ibid., 65; Gene Sharp, *From Dictatorship to Democracy: A Conceptual Framework for Liberation,* 4th ed. (East Boston, MA: Albert Einstein Institution, 2010).

[30] J.F.C. Fuller, *The Generalship of Alexander the Great* (London: Eyre and Spottiswood; 1958), 277-278, quoted in Asprey, vol. 1, 7-8. The overall concept of *Homonoia* is presented as a belief in the unity of mankind, but the author asserts that it is more likely Alexander's shrewd political sense to win various tribes to his side. Regardless, this concept provides historical context to the importance of influence in the human domain; COL T. A. Dodge, *Hannibal,* vol. 1 (Boston, MA: Houghton Mifflin, 1891), 176, quoted in Asprey, vol. 1, 7-8.

[31] Thomas E. Lawrence, *Seven Pillars of Wisdom: A Triumph* (New York: Penguin Books, 1986).

[32] Dixee R. Bartholomew-Feis, *The OSS and Ho Chi Minh: Unexpected Allies in the War Against Japan* (Lawrence: University Press of Kansas, 2006), 317.

[33] Ibid., 398. Allison Thomas interview with Dixee Bartholomew-Feis.

[34] "Full Transcript of 1997 OSS/Viet Minh Meeting," 61-97, quoted in Dixee R. Bartholomew-Feis, *The OSS and Ho Chi Minh: Unexpected Allies in the War Against Japan* (Lawrence: University Press of Kansas, 2006), 398. In an interview with Dixee Bartholomew-Fies, MAJ White recalled the evening: "The dinner was a horror. The French confined themselves to the barest minimum of conversation and scarcely spoke to the Chinese, who were quickly becoming drunk . . . At one point I spoke to Ho very quietly. 'I think, Mr. President, there is some resentment over the seating arrangement at this table.' I meant, of course, my place next to him. Ho thought for a moment, then replied simply: 'Yes, I can see that, but who else could I talk to?'."

[35] JCS, JP 3-12, I-5.

[36] Ibid., v.

[37] Ibid., I-2.

[38] Ibid.

[39] Ibid.; Headquarters, Department of the Army (HQDA), Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: Government Printing Office, 2017), 1-13.

[40] Ibid., 1-12.

[41] JCS, JP 3-12, I-3.

[42] Ibid.

[43] Ibid., I2-I3

[44] Ibid., II-1

[45] Ibid., II-2.

[46] HQDA, FM 3-12, 1-9.

[47] Romano, 37-38.

[48] Michael S. Rogers, "A Challenge for the Military Cyber Workforce," *Military Cyber Affairs* 1, no. 1 (2015): article 2, accessed April 25, 2017, http://scholarcommons.usf.edu/mca/vol1/iss1/2.

[49] JCS, JP 5-0, x.

[50] This is the author's personal observation and assertion.

[51] Department of the Army, Headquarters U.S.Army Training and Doctrine Command, "TRADOC: Designing & Building the Future Army: Command Overview" (PowerPoint Presentation, Training and Doctrine Command, Fort Eustis, VA, 2014), accessed April 16, 2016, http://www.tradoc.army.mil/SitewideContent_TRADOC/Docs/TRADOCCommandOverview.pdf, 4.

[52] Patrick M. Duggan, "Why Special Operations Forces in US Cyber-Warfare?" *Cyber Defense Review*, January 8, 2016, accessed June 6, 2017, http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/, para. 2.

[53] Duggan, “Strategic Development of Special Warfare in Cyberspace,” 46-52.

[54] Birtle, 232-233.

CHAPTER 3

RESEARCH METHODOLOGY

The purpose of this study is to explore how USSOCOM should employ special warfare in and through cyberspace and enable success in the human domain across the range of military operations. In his address to the United States Army Command and General Staff College, General David Perkins emphasized the importance in defining "why you're doing" before "what you do."[1] Special warfare operational art and the conceptual application of special warfare in and through cyberspace must address special warfare's contribution to operational art in the human domain. Considering the context of special warfare's contribution to operational art, a study that addresses the explanations of human action as a second/third order effect of CE-SW may provide insight into a framework of analysis in developing special warfare operations in and through cyberspace.

Chapter 3 discusses the context of the content analysis model that is used in chapter 4 to explore the use of CE-SW and its proposed effect in the human domain. In this model, CE-SW conceptually explored through a qualitative content analysis and then uses Craig Parsons's typology of explanations of human actions to examine effects within the human domain. By understanding special operations placement and access to affect the human domain through the various typologies, existing theories to social sciences may highlight correlations to justify approaches developed during operational design. Inherent in this analysis is the realization that the military is only one element of the instruments of national power, and strategic commanders and staffs must understand how

to collaborate and leverage the other instruments of national power in achieving unity of effort.

Research Method and Design Appropriateness

Rationale for Research Method

A qualitative content analysis method was used in this study to facilitate the collection, analysis, and interpretation of the conceptual application of special warfare operations and cyberspace operations with their effects in the human domain using a typology for human action. Content analysis research allows the researcher to analyze written and visual contents to examine the conscious and unconscious beliefs, attitudes, values and ideas of people and groups.[2] This particular study examines existing literature, independent studies, and doctrine as a source of the content of the analysis. In conducting the content analysis, it allows the researcher to determine relevant categories to identify and analyze to provide some explanatory power in their particular area of research.[3] The relevant categories in this study seek to address the apparent operational gap regarding USSOCOM's application of cyberspace operations to enable special warfare in the human domain. This study is similar to previous works regarding the linkages between special warfare operations and cyberspace operations and their inherent relationship with the human domain.[4] This study expands on the effects of cyberspace operations to enable special warfare by analyzing their implications in the human domain through a typology for human action.

Rationale for Research Design

Within the context of special warfare, the concept of either stabilizing or destabilizing seeks to not only change the environment, but to change individual perceptions of the environment. Individual perception of the environment shapes the construction of relationships between the incumbent government or the insurgent and the people. Within the context of Stathis Kalyvaas's zones of control,[5] by shaping the perceived relationship construction, special warfare may be in a position to influence the human domain in and through cyberspace. The use of cyberspace has increasingly affected the information environment and altered the social construction of societal norms. The qualitative content analysis addresses research questions 1 and 2 by examining the current application of operational art in executing special warfare campaigns and determining how USSOCOM can integrate cyber-enable special warfare. As special warfare's primary contribution to operational part is in the human domain, a typology for human action is used to answer research question 3. Craig Parsons developed this particular typology for human behavior to organize political science literature by classes of substantive causes for human action. The basic claims stem from either a logic of position or a logic of interpretation.[6]

Summary

Chapter 3 discusses the application of a qualitative content analysis study to address USSOCOM's integration of CE-SW to enable success in the human domain across the range of military operations. The content analysis provides a credible model in analyzing the current application of special warfare and its contribution to operational art and exploring the integration of CE-SW. Success in special warfare is dependent on

enabling success in the human domain; the proposed typology for human action provides direct linkage to contemporary political science literature. The four claims offer an alternative perspective in analyzing how populations may be primed and queued for action.

---

[1] GEN David Perkins, Speech, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2017.

[2] Wallen and Fraenkel, 408.

[3] Ibid.

[4] Duggan, "Strategic Development of Special Warfare in Cyberspace," 46-53; Duggan, "Man, Computer, and Special Warfare."

[5] Stathis N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge, UK: Cambridge University Press, 2011), 196, 211-213.

[6] Craig Parsons, *How to Map Arguments in Political Science* (Oxford, England: University Press, 2007), 11-16.

CHAPTER 4

ANALYSIS

Important Notes

The purpose of this qualitative content analysis study was to examine USSOCOM's current incorporation of cyberspace operations to enable success in the human domain across the range of military operations. To address this perceived gap, this study examined historic and contemporary literature from both the special warfare and cyberspace operations perspectives to determine areas of overlapping equities. This examination and resulting determinations involved the use of a typology for human action in examining how cyberspace operations and special warfare operations in and through cyberspace can shape the human domain across the range of military operations. Intelligence preparation of the environment provides insight into underlying factors that may prime or queue individuals or groups to behave in a particular manner. As seen in chapter 2, special warfare operations provide a catalyst to exploit these underlying factors to stabilize or destabilize the operational environment to meet theater and national strategic objectives.

Chapter 4 begins with a general discussion regarding the incorporation of cyberspace operations and a CEMA operations process within the context of special warfare. Two research questions (1 and 2) are presented and followed by a qualitative content analysis leading to actions that USSOCOM can support to seamlessly integrate cyberspace operations and special warfare operations in and through cyberspace. The third research question uses the typology for human action as an approach to understanding how individuals and groups may be queued or primed for particular human

behavior and how CE-SW can magnify the effects of underlying factors in the operational environment to facilitate success in the human domain.

Is the Current Application of Operational Art Suitable for Executing Special Warfare in and through Cyberspace?

The present application of operational art is suitable for implementing special warfare in and through cyberspace. Some literature does highlight that failure to address the strategic gap in CE-SW will contribute to a widening strategic capabilities gap.[1] CE-SW is a tactical application of capabilities with strategic effect. If the U.S. military fails to integrate special warfare and cyberspace operations to compete with Russian and Iranian efforts, the United States may be at a disadvantage. The *National Security Strategy*, the *National Military Strategy*, and the *Cyber Defense Strategy* provide the strategic ends to address the growing concerns within cyberspace.[2] The overarching guidance in these three strategic documents is sufficient as strategic ends to integrate special warfare and cyberspace operations.

Joint doctrine provides the framework of analysis through the joint operation planning process to account for operational variables, especially with human action. Through the use of cyberspace, special warfare campaigns are poised to address growing methods to interact with the operational environment. As stated in this study, when conducting a center of gravity analysis, traditional application focuses primarily on friendly and enemy centers of gravity. Center of gravity analysis in a special warfare campaign must address partner forces and other relevant actors' centers of gravity. Although not particularly discussed, joint doctrine does include neutral relevant actors during the operational variable analysis, but they are not addressed within a center of

gravity analysis.[3] Joint operating concepts do address human aspects of military operations and offer the perspective through a temporal lens; however, the nature of these concepts only recommend that services consider relevant actors and their contribution.[4]

As previously acknowledged, special warfare has an inherent reliance on the human domain. Special warfare's contribution to operational art is within the human domain. When planning for a special warfare campaign, the current application of operational art is sufficient, but planners must recognize the inherent relationships and sustained engagement through special warfare. Through continued engagement, special warfare provides situational awareness, influence, and partner capacity. Situational awareness and influence are more holistically tied to the operational environment at large, where partner capacity directly contributes to partner force warfighting capacity.

There are moderate indications that collaboration between the two doctrinal centers of special warfare and cyberspace operations is taking place. However, most special operations doctrine needs specific revisions to further address the incorporation of cyber and electromagnetic operations and special warfare. Special operations leadership emphasizes the need to continue developing education to address social movement and cyberspace tools and methods to enable special warfare.[5] A former commander of USCYBERCOM stated the need to develop collaboration across the whole of government to develop more interdependent processes and concepts that streamline the application of cyber electromagnetic effects.[6] The leadership of both operational communities indicate that they understand the importance of collaboration and integrating mutually supporting operations to support joint force commanders and U.S. embassy country teams. The implications of continued collaboration suggest sufficient

direction from the U.S. President in the *National Security Strategy*.[7] Strategic military leaders' application of operational art and continued development of cyberspace operations across the whole government demonstrate the linkages of ends, ways, and means.

At the time of the study, there were limited instances of incorporating cyber electromagnetic operations within contemporary overarching special warfare doctrine. JP 3-05 discusses some application of cyberspace operations but is only limited to the protective function of cybersecurity and cyberspace operations support. The JP goes on to discuss electronic warfare and the integration of it to help the commanders' decision-making process while referencing the overarching cyberspace operations in electronic warfare doctrine.[8] Considering the overarching aspect of this publication, the integration of cyberspace operations and special operations in and through cyberspace are necessary to support considerations for special operations forces that should be updated within chapter 4 of this publication. Although limited discussions within this publication address the integration of cyber electromagnetic operations and special operations, there are several trends that highlight overlapping processes to include intelligence support and operational preparation of the environment that are explored below.

With limited discussion other than Colonel Duggan's works regarding CE-SW, it is prudent to explore overlapping concepts between special warfare operations and cyber electromagnetic operations. Considering special warfare's persistent engagement, special warfare campaigns contribute to the joint intelligence preparation of the operational environment. Cyberspace operations, specifically cyberspace ISR and cyberspace OPE, may support intelligent preparation of the operational environment. Understanding the

placement of special operations forces and access to cyberspace operations, joint planning between special operations and cyberspace operations may create additional opportunity and staff synergy to further contribute to the intelligence preparation of the operational.

Special warfare and cyberspace operations provide situational awareness and clarity that contribute to the national level perspective across the whole of government. Based on the application of special warfare and CEMA operations, their contribution to operational art enables theater and national strategic perspectives that support joint force commander's strategic objectives. They also support U.S. embassy country teams' strategic goals through a whole of government approach. Special warfare and cyberspace operations are developed at the strategic level and involve strategic level decisions but have tactical level execution. The tactical execution of special warfare and CEMA, in turn, has operational and strategic level effects.

Special operations and cyberspace operations contribute to the joint intelligence preparation of the environment through intelligence operations. The physical network layer of cyberspace is a primary target for signals intelligence.[9] The application of signals intelligence across special warfare operations is an inherent part of CEMA and must undergo consideration for special warfare planners. As USSOCOM continues to seek effects in cyberspace, it is important that planners do not attempt to create capabilities or operate beyond what has been delegated by other government agencies.

Cyberspace operations and special operations conduct operational preparation of the environment.[10] The contextual application and contrast between special operations in cyberspace operational preparation of the environment differ with intent, methods, and

authorities. Although the preponderance of this discussion extends beyond the scope of the study, operational preparation of the environment is one overlapping application where early considerations regarding conceptual planning and operational planning may provide mutually beneficial results from operations.

How Can/Should Cyberspace Operations Be Employed to Support Special Warfare in and through Cyberspace?

When addressing how special warfare can leverage the use of cyberspace and consider cyberspace operations to support special warfare, existing conventional processes provide linkage to integrating these conceptually. Current doctrine provides the conceptual application of CEMA working groups at echelons above battalion.[11] Commanders and staff have the doctrinal foundation to integrate cyberspace operations and special warfare through existing processes as organizations refine CEMA processes.

In the same way that aircraft is requested to provide an effect, CEMA should be viewed in the same manner. As an operational commander, mission requirements and effects provide CEMA planners with task and purpose. The means by which CEMA are conducted should be transparent to the supporting force, provided the capability does not currently exist within their task organization.

USSOCOM has an existing architecture that facilitates electronic warfare and signals intelligence. By exploring this existing relationship where aspects of electronic warfare and signals intelligence are delegated to special operations from other agencies, the military intelligence detachment within a special operations time may logically nest with the development of tactical cyberspace operations that may be delegated in the future. Signals intelligence was largely a strategic asset during World War II and further

developed and used operationally during operations in Vietnam.[12] Although the existing architecture may facilitate the organizational development, special warfare's contribution to operational art is within the human domain, and CE-SW should have effects within the human domain.

How Can Cyberspace Operations Strengthen Special Warfare in Influencing the Human Domain?

As previously stated, special warfare's contribution to operational art takes place in the human domain. Within the joint operations planning process and the military decision-making process, operational variables are the standard framework for evaluating the operational environment. In the joint environment, additional analysis uses a Clausewitzian framework to explore and evaluate enemy and friendly centers of gravity.[13] From an academic perspective, often these centers of gravity studies only address issues at face value. For example, most contemporary literature regarding center of gravity analysis discusses the people as the center of gravity with a little in-depth analysis into a typology for human behavior that seeks to understand how a particular population may be primed for human behavior. From a political and social science perspective, operational variables as a planning tool merely facilitate the collection and consumption of data regarding the environment; however, they do not facilitate linkages to contemporary political science literature regarding empirical claims.

To address research question three, this study offers evaluating effects of special warfare through the lens of a typology for human behavior. This typology is grounded in the works of Parsons to address claims within academic literature to explain political science claims.

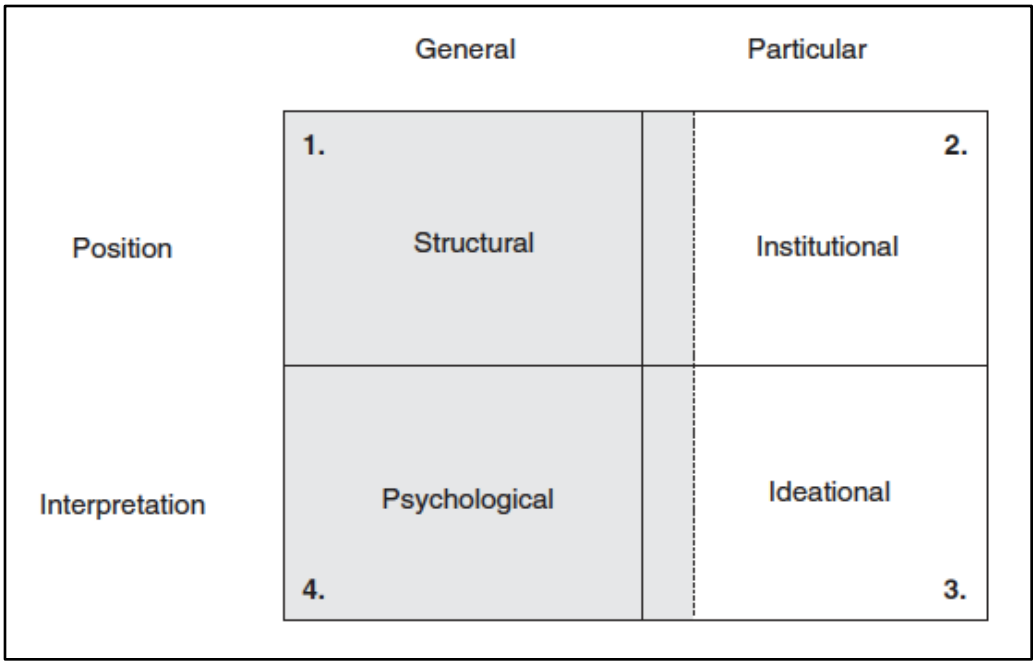

Figure 3. Fundamental Matrix of Explanations of Action

Source: Craig Parsons, *How to Map Arguments in Political Science* (Oxford, England: University Press, 2007), 15.

Logics of Position

Structural Claims

Structural claims represent an application that explains human action as an individually rational function of a logic of position and in a material landscape. A material landscape represents an obstacle of shifting and subjective influence in a given environment. Some theories include Marxism, economic liberalism, and realism.[14]

Institutional Claims

Institutional claims explain action by pointing to someone's position within a man-made and intersubjectively present obstacle course where institutions exercise some

range of causal autonomy.[15] An example of institutional claims is represented in a democratic process, where an individual's preference may be overridden by their institutional relationship with a democratic party.

From an operational and strategic perspective, operational variables help frame the understanding of how individuals or groups are positioned in the operational environment. Using a typology for human action, everyday use of cyberspace presents an opportunity to influence the manner in which the population interacts individually and collectively. Understanding that special warfare seeks to stabilize or destabilize an operational environment, existing structural relationships and institutional ties can be influenced through CE-SW.

Given the nature of structural claims, the use of cyberspace impacts the social construction of the operational environment through the use of cyber personas. Acknowledging the ambiguity of cyber personas, the social structure within the operational environment may influence all four typology claims. However, the use of cyberspace does create opportunity given the nature of interaction of individuals and groups within cyberspace and how relationships are constructed. These relationships may be with persons, groups, or institutions.

By looking through the lens of institutional claims and understanding operational variables, this approach provides additional context to human action. In the same way that cyberspace has created opportunities to influence social construction, an individual or group operating within an institutional framework may be more predisposed to a particular human action. The use of cyberspace creates an opportunity to influence the human domain through understanding institutional claims. Some examples may be the

use of cyberspace operations in support of special warfare to degrade or enhance institutional resiliency or public perception of a particular institution. In this case, a cyberspace action may only provide or limit access while enabling intelligence operations or information operations. Alternatively, a human action may be triggered by the application of cyberspace operations based on an individual's position within an institution or interaction of cyber personas.

Logics of Interpretation

Psychological Claims

Psychological claims describe human action through interpretation of causal effects due to hardwired mental processes that fall outside a simple rational application. This claim accounts for irrational decision-making as a result of psychological traps to include biases, misinterpretations, instincts or effects.[16]

Ideational Claims

Ideational claims categorize human action by linking them to elements to include practices, symbols, norms, grammars, models, beliefs and/or through how certain people interpret their world.[17] One way to conceptualize these claims is through understanding Geert Hofstede's cultural onion model.[18]

In contrast to logics of position, logics of interpretation may fall outside of a planner's rational understanding of human behavior. Individuals and groups within the operational environment may lack the situational awareness to understand psychological traps that they may be exhibiting. These psychological traps may be indicative of

hardwired mental processes within psychological claims or through cultural conditioning within ideational claims.

Through understanding operational variables and how individuals interact through cyberspace, logics of interpretation influence psychological and ideational approaches. One difficulty in amplifying claims within logics of interpretation is entirely extrapolating a person's or group's perception and how that triggers primarily psychological human action. Some operational environments may have cultural underpinnings that prime and queue individuals and groups for human action. In this case, the desired effect to stabilize or destabilize an operational environment may use cyberspace to produce an effect that is closely tied to underlying cultural and ideational factors. Overall, it is important that the operational variables define the operational environment and a typology for human action shape the approach to influence the human domain. This particular typology provides that linkage from operational variables to qualitative and quantitative literature in political science to develop strategies to integrate cyberspace operations and special warfare.

Summary

Chapter 4 provides the observations of the qualitative content analysis conducted to answer the research questions. Overall, the application of special warfare and its contribution to operational art are appropriate to integrate special warfare and cyberspace operations. With special warfare's contributions to operational art being in the human domain, a typology for human action provides unique insight into understanding how the human domain may be primed and queued human action. The application of operational art in existing literature demonstrates initiatives to integrate cyberspace and special

warfare operations, through linking the three components strategy. Existing relationships of electronic warfare and signals intelligence within special operations provide a foundation for CE-SW.

---

[1] Duggan, "Strategic Development of Special Warfare in Cyberspace," 52.

[2] U.S. President, *The National Security Strategy 2015* (NSS) (Washington, DC: The White House, 2015); Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (Washington, DC: Department of Defense, 2015). The NSS and NMS discuss the national and strategic nature of cyberspace and discuss strategic ends.

[3] JCS, JP 5-0, III-8.

[4] Vice Chairman Joint Chiefs of Staff, *Joint Concept for Human Aspects of Military Operations* (Washington, DC: Joint Chiefs of Staff, 2016), 7-8.

[5] Votel et al., 108.

[6] Rogers, 1.

[7] The White House, NSS. The 2015 NSS addresses the growing need to combat cyber threats in multiple contexts throughout the document.

[8] JCS, JP 3-05, 82, 85-86.

[9] JCS, JP 3-12, I-3.

[10] JCS, JP 3-05, II-4-5; JCS, JP 3-12, II-5.

[11] HQDA, FM 3-12, 3-3.

[12] Frederick W. Winterbotham, *The Ultra Secret* (New York: Haper & Row, Publishers, 1974); Robert J. Hanyok, *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975* (Washington, DC: National Security Agency: Center for Cryptological History, 2002), accessed June 6, 2017, http://www.fas.org/irp/nsa/spartans/index.html, xi.

[13] JCS, JP 5-0, III-8.

[14] Parsons, 39.

[15] Ibid.

[16] Ibid., 39-40.

[17] Ibid., 40.

[18] Bob Waisfisz, “An Organisational Cultural Perspective,” *Geert-Hofstede*, accessed June 6, 2017, https://geert-hofstede.com/tl_files/art%20organisational%20culture%20perspective.pdf, 1-3.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Overall, the current application of operational art is suitable for executing special warfare in and through cyberspace. If the United States fails to integrate special warfare and cyberspace operations across the whole of government, it will contribute to a widening strategic capabilities gap by allowing adversaries to gain a strategic advantage in cyberspace. Cyberspace operations and CE-SW should support special warfare campaigns' contribution to operational art in the human domain.

Through sustained engagement, special warfare campaigns connect tactics to strategy through situational awareness, influence, and capacity building. Cyberspace operations can strengthen special warfare in shaping the human domain by complementing underlying factors that prime and queue human behavior. An operational application is varied by context but should address existing academic claims representative of the operational environment by a thorough examination of operational variables and centers of gravity.

The particular typology for human behavior used in this study merely provides a framework for analysis within the context of operational planning. Existing processes conduct analysis through the use of operational variables that provide a logical and contextual understanding of the environment. This particular typology provides linkage to existing political science literature. As methods and techniques for integration of cyberspace operations and special warfare are developed, the contribution to operational art in the human domain can be explored through the use of this typology.

Recommendations

This study examines the apparent gap with integrating cyberspace operations and special warfare. As USCYBERCOM continues to develop their growing force structure, USSOCOM should explore using existing internal force structure as a foundation to conduct special warfare in and through cyberspace. Continued collaboration between the U.S. Army Cyber Center of Excellence and the U.S. Army Special Operations Center of Excellence should also address gaps in existing doctrine, organization, training, materiel, leadership and education, personnel, and facilities. There may be overlap in existing force management requirements between conventional military and special operations; however, deliberate efforts should address the unique special operations requirements to operate in and through cyberspace. As conscious efforts are explored to support integration and improve force structure, below are some refined areas for additional research.

Doctrine Review

As stated in the study there are some parallels that Andrew Birtle highlighted in his work in the difficulties proliferating counterinsurgency doctrine. By evaluating the development of counterinsurgency doctrine, some best practices and lessons learned may provide insight into developing logical solutions for the development of cyberspace doctrine. Regardless, USSOCOM should conduct a doctrine review, specifically in collaboration with USCYBERCOM to account for gaps in current doctrine. The refinement process for contemporary doctrine will inform leader development for the integration of CE-SW.

Leader Development

The Army Leader Development Model emphasizes the three pillars of leader development: training, education, and experience.[1] Refined doctrine must be the input to inform the training and education processes as USCYBERCOM and USSOCOM determine requirements to fill apparent gaps. USSOCOM must balance the need to develop unique special operations capabilities and potentially create schools to fill capability gaps, in conjunction with other government agency equities in mind. Once training and education provide a foundation to integrate CE-SW, combat training centers and operational environments will foster the environment to further refine processes of integration.

Organization

Resident knowledge of cyberspace within existing force structure, such as military intelligence, electronic warfare, and signal personnel, should be leveraged to integrate CEMA planning and support special warfare campaigns. An active CEMA working group incorporated into special operations planning processes may further identify gaps to streamline integration. USSOCOM CEMA integration should be employed through combat training centers and operationally to support continued evaluation and development. In doing so, it may be prudent to develop a collaborative USCYBERCOM and SOCOM concept, operating in and through cyberspace or simply update existing operating concepts to better address the integration of special operations in and through cyberspace.

USASOC recently restructured the 75th Ranger Regiment by adding a Military Intelligence Battalion that includes a CEMA company.[2] The Ranger Regiment supports

surgical strike within USASOC, and this development of a CEMA company may streamline a solution to integrate CEMA into special warfare. Overall, the organizational changes within the Ranger Regiment do indicate the importance USASOC is placing on accounting for gaps in integrating cyberspace operations across Army special operations.

Additional Research Areas

Given the context of this study, several applications and tactical evaluations of integrating cyberspace operations and special warfare exceed the classification of this study. One area for recommended additional research is the observation of tactical integration of cyberspace operations and special warfare. These observations should evaluate the application of a typology for human behavior to support special warfare. This particular typology is not exclusive to CE-SW but can be applied holistically to exploring new methods in conducting special warfare campaigns. Observations can be performed at selected training events and combat training centers. The research of this study did provide access to some of these observations; however, contribution beyond the study requires additional study and consideration.[3]

Given the strategic development of electronic warfare and signals intelligence during World War II and Vietnam, additional research into the development of Army security agency special operations detachments may be a worthwhile endeavor to evaluate means to incorporate CE-SW at the tactical level. Given the nature of the subject matter, this additional research also exceeds the classification of this study.

---

[1] Headquarters, Department of the Army, *Army Leader Development Strategy* (Washington, DC: Government Printing Office, 2013), 8.

[2] Marty Skovlund Jr., "The 75th Ranger Regiment is Adding a Fifth Battalion," *Task and Purpose*, May 17, 2017, accessed June 1, 2017, http://taskandpurpose.com/75th-ranger-regiment-adding-fifth-battalion, para. 7.

[3] For further research, contact the Center for Army Lessons Learned and the USASOC Lessons Learned.

BIBLIOGRAPHY

Books

Aid, Matthew M. *The Secret Sentry: The Untold History of the National Security Agency.* New York: Bloomsbury Press, 2010.

Andrew, Christopher, Richard J. Aldrich, and Wesley K. Wark, eds. *Secret Intelligence: A Reader*. New York: Routledge, 2009.

Asprey, Robert B. *War in the Shadows: The Guerrilla in History*. Vol. 1. Lincoln, NE: IUniverse, 2002.

_____. *War in the Shadows: The Guerrilla in History*. Vol. 2. Lincoln, NE: IUniverse, 2002.

Bank, COL Aaron. *From OSS to Green Berets: The Birth of Special Forces.* New York: Simon and Schuster, 1986.

Bartholomew-Feis, Dixee R. *The OSS and Ho Chi Minh: Unexpected Allies in the War Against Japan*. Lawrence: University Press of Kansas, 2009.

Birtle, Andrew J. *U.S. Army Counterinsurgency and Contingency Operations Doctrine, 1942-1976.* Washington, DC: Center for Military History U.S. Army, 2006.

Boot, Max. *The Savage Wars of Peace: Small Wars and the Rise of American Power*. New York: Basic Books, 2014.

Clausewitz, Carl Von. *On War*. Translated by Michael Howard and Peter Paret. Oxford, England: Oxford University Press, 2007.

Kalyvas, Stathis N. *The Logic of Violence in Civil War*. Cambridge, UK: Cambridge University Press, 2011.

Lawrence, Thomas E. *Seven Pillars of Wisdom: A Triumph*. London: Penguin Books, 2000.

Nye, Joseph S. *The Future of Power*. New York: Public Affairs, 2011.

Paddock, Alfred H., Jr. *Special Warfare: Its Origin*. Lawrence: University Press of Kansas, 2002.

Paret, Peter, Gordon Alexander Craig, and Felix Gilbert. *Makers of Modern Strategy: From Machiavelli to the Nuclear Age.* Princeton, NJ: Princeton University Press, 1986.

Parsons, Craig. *How to Map Arguments in Political Science*. Oxford, England: University Press, 2007.

Petit, Brian S. *Going Big by Getting Small: The Application of Operational Art by Special Operations in Phase Zero*. Denver, CO: Outskirts Press, 2013.

Schneider, James J. *Guerrilla Leader: T.E. Lawrence and the Arab Revolt*. New York: Bantam Books, 2011.

Sharp, Gene. *From Dictatorship to Democracy: A Conceptual Framework for Liberation*. 4th ed. East Boston, MA: Albert Einstein Institution, 2010.

Wallen, Norman E., and Jack R. Fraenkel. *Educational Research: A Guide to the Process*. Mahwah, NJ: Taylor and Francis [CAM], 2001. Accessed April 16, 2017. EBSCOhost.

Winterbotham, Frederick W. *The Ultra Secret*. New York: Harper and Row, 1974.

Yarger, Harry R. *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2006.

Zimmerman, Dwight Jon., and John Gresham. *Beyond Hell and Back: How Americas Special Operations Forces Became the World's Greatest Fighting Unit*. New York: St. Martins Griffin, 2008.

Government Documents

Department of the Army, Headquarters U.S.Army Training and Doctrine Command. TRADOC Pamphlet 525-8-5, *The U.S. Army Functional Concept for Engagement*. Washington, DC: Fort Eustis, VA, 2014.

Headquarters, Department of the Army. Army Doctrine Publication 3-05, *Special Operations*. Washington, DC: Government Printing Office, 2012.

_____. Army Doctrine Reference Publication 2-0, *Intelligence*. Washington, DC: Government Printing Office, 2012.

_____. *Army Leader Development Strategy*. Washington, DC: Government Printing Office, 2013.

_____. Field Manual 3-05.102, *Army Special Operations Intelligence*. Washington, DC:

_____. Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*. Washington, DC: Government Printing Office, 2017.

_____. *The National Military Strategy of the United States of America*. Washington, DC: Department of Defense, 2015.

_____. Joint Publication 3-05, *Special Operations*. Washington, DC: Department of Defense, 2014.

_____. Joint Publication 3-12, *Cyberspace Operations*. Washington, DC: Department of Defense, 2013.

_____. Joint Publication 5-0, *Joint Operational Planning*. Washington, DC: Department of Defense, 2011.

U.S. Congress. House. Report 118-840, *National Defense Authorization Act for Fiscal Year 2017*. Conference Report to Accompany HR S. 2943. Washington, DC: November 30, 2016. Accessed July 30, 2017. https://www.congress.gov/congressional-report/114th-congress/house-report/840/1.

U.S. President. *The National Security Strategy 2015*. Washington, DC: The White House, 2015.

Vice Chairman Joint Chiefs of Staff. *Joint Concept for Human Aspects of Military Operations*. Washington, DC: Joint Chiefs of Staff, 2016.

Journals/Periodicals

Cleveland, LTG (RET), Charles T., MG James B. Linder, and CW4 Ronald Dempsey. "Special Operations Doctrine: Is it Needed?" *PRISM: Special Operations in a Chaotic World* 6, no. 3 (2016): 5-19.

Duggan COL, Patrick Michael. "Strategic Development of Special Warfare in Cyberspace." *Joint Forces Quarterly*, no. 79 (4th Quarter 2015): 46-53. Accessed June 6, 2017. http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/Article/621123/strategic-development-of-special-warfare-in-cyberspace/.

_____. "Man, Computer, and Special Warfare." *Small Wars Journal* (January 4, 2016). Accessed June 6, 2017. http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

_____. "Why Special Operations Forces in US Cyber-Warfare?" *Cyber Defense Review*, January 8, 2016. Accessed June 6, 2017. http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/.

Duggan COL, Patrick M., and Elizizabeth Oren. "U.S. Special Operations Forces in Cyberspace." *The Cyber Defense Review* 1, no. 2 (Fall 2016): 73-79. Accessed December 17, 2016. http://cyberdefensereview.army.mil/The-Journal/Current-Issue/.

Kapusta CAPT Philip. “The Gray Zone.” *Special Warfare* 28, no. 4 (October 2015): 18-25. Accessed June 6, 2017. http://www.soc.mil/SWCS/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf.

Rogers, Michael. “A Challenge for the Military Cyber Workforce.” *Military Cyber Affairs* 1, no. 1 (2015): article 2. Accessed April 25, 2017. http://scholarcommons.usf.edu/mca/vol1/iss1/2.

Skovlund, Marty, Jr. “The 75th Ranger Regiment is Adding a Fifth Battalion.” *Task and Purpose*, May 17, 2017. Accessed June 1, 2017. http://taskandpurpose.com/75th-ranger-regiment-adding-fifth-battalion/.

Votel, GEN Joseph L., LTG (RET) Charles T. Cleveland, COL Charles T. Connet, and LTC (RET) Will Irwin. “Unconventional Warfare in the Gray Zone.” *Joint Forces Quarterly*, no. 80 (1st Quarter 2016): 101-109. Accessed June 6, 2017. http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

Waisfisz, Bob. “An Organisational Cultural Perspective.” *Geert-Hofstede*. Accessed June 6, 2017. https://geert-hofstede.com/tl_files/art%20organisational%20culture%20perspective.pdf.

Williams, MG Brett T. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Forces Quarterly*, no. 73 (2nd Quarter 2014): 12-19. Accessed June 6, 2017. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf?ver=2014-04-01-122156-563.

Online Sources

The American Presidency Project. “President John F. Kennedy Remarks at West Point to the Graduating Class of the U.S. Military Academy, West Point, NY, June 6, 1962.” Accessed July 30, 2017. http://www.presidency.ucsb.edu/ws/?pid=8695.

Army Capabilities Integration Center. *Multi -Domain Battle: Combined Arms for the 21st Century*. U.S. Army. Accessed June 6, 2017. http://www.arcic.army.mil/App_Documents/Multi_Domain_Battle.pdf.

Pomerleau, Mark. “Congress Set to Elevate CYBERCOM to Unified Combatant Command.” C4ISRNET, December 2, 2016. Accessed June 6, 2017. http://www.c4isrnet.com/articles/congress-authorizes-elevating-cybercom-to-unified-combatant-command.

U.S. Special Operations Command. “SOF Imperatives.” U.S. Army, 2017. Accessed March 28, 2017. http://www.soc.mil/USASOCHQ/SOFImperatives.html.

Papers/Reports

Anderson, MAJ Talon G. “Adapting Unconventional Warfare Doctrine to Cyberspace Operations: An Examination of Hacktivist Based Insurgencies.” Master’s thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2014.

Eidman, Christopher R., and Gregory Scott Green. “Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare.” Master’s thesis, Naval Postgraduate School, Monterey, CA, 2014.

Hanyok, Robert J. *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975*. Washington, DC: National Security Agency: Center for Cryptological History, 2002. Accessed June 6, 2017. http://www.fas.org/irp/nsa/spartans/index.html.

Leed, Maren. *Offensive Cyber Capabilities at the Operational Level: The Way Ahead.* Washington, DC: Center for Strategic & International Studies, 2013.

Madden, Dan, Dick Hoffman, Michael Johnson, Fred T. Krawchuk, Bruce Nardulli, John E. Peters, Linda Robinson, and Abby Doll. *Toward Operational Art in Special Warfare*. Santa Monica, CA: Rand Corporation, 2016.

Romano, COL Kevin P. “Army Cyber Mission Force: Ambitions and Realities.” Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2015.

U.S. Special Operations Command. *Operating in the Human Domain*. McDill Air Force Base, FL: Headquarters, U.S. Special Operations Command, 2015.

National Security Agency/Central Security Service. “Operation Starlight: A SIGINT Success Story.” FOIA Case #7319, undated. Accessed July 30, 2017. https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/operation_starlight.pdf.

Other Sources

Department of the Army, Headquarters U.S.Army Training and Doctrine Command. “TRADOC: Designing & Building the Future Army: Command Overview.” PowerPoint Presentation, Training and Doctrine Command, Fort Eustis, VA, 2014. Accessed April 16, 2016. http://www.tradoc.army.mil/SitewideContent_TRADOC/Docs/TRADOCCommandOverview.pdf.

Perkins, GEN David. Speech, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2017.