The Development of Operational Art and CEMA in Multi-Domain Battle during the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016

A Monograph

by

MAJ Ronald W. Sprang
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
24-05-2018	Master's Thesis	JUN 2017- MAY 2018

4. TITLE AND SUBTITLE
The Development of Operational Art and CEMA in Multi-Domain Battle during the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Ronald W. Sprang, USA

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 ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Military Studies Program

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

The current operational environment and the emerging challenges of near peers and non-state actors have combined to create a challenge for the United States to gain and maintain the advantage across all three levels of war and across all domains. Russia, China, North Korea, and Iran have developed and implemented varying levels of cyber capabilities in support of their strategic national objectives. The Russian 'New Generation Warfare' has evolved to the 'New-Type of War' applying operational art as a means to gain an asymmetric advantage over an enemy's technological advantage. Fundamental to gaining this advantage is the employment of cyberwarfare.

The Army's multi-domain battle concept outlines emerging requirements for the military to achieve effects in the contemporary operational environment against emerging near peer threats. Cyber capabilities are critical to enable operational commanders the opportunity to create temporary windows of advantage, shape the deep fight, control tempo of multi-domain operations, and arrange cyber effects in time and space to achieve strategic objectives. Both case studies, the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016, demonstrate cross domain synergy achieved with successful application of cyber electromagnetic activities (CEMA) to provide opportunities during multi-domain operations.

The significance of this research is that it contributes to an understanding of cyberwarfare as applied through the lens of operational art and multi-domain battle. The study provides a conceptual framework to assist in answering two key questions. First, how do military forces offensively and defensively employ cyber capabilities? Second, how can the US Army develop an operational approach to gain an advantage in the cyber domain and synergy across other domains to create windows of advantage?

15. SUBJECT TERMS
Cyberwarfare, Multi-Domain Battle, Guadalcanal, Russian Operations Ukraine, Operational Art, Cross-Domain Synergy, 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**			Major Ronald W. Sprang
Unclassified	Unclassified	Unclassified	Unclassified	64	**19b. TELEPHONE NUMBER** *(include area code)* 913-526-2283

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

Monograph Approval Page

Name of Candidate: MAJ Ronald W. Sprang

Monograph Title: The Development of Operational Art and CEMA in Multi-Domain Battle during the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016

Approved by:

_____, Monograph Director
Bruce E. Stanley, PhD

_____, Seminar Leader
Jeffrey S. Davis, COL

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 24th day of May 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

The Development of Operational Art and CEMA in Multi-Domain Battle during the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016, by MAJ Ronald W. Sprang, US Army, 65 pages.

The current operational environment and the emerging challenges of near peers and non-state actors have combined to create a challenge for the United States to gain and maintain the advantage across all three levels of war and across all domains. Russia, China, North Korea, and Iran have developed and implemented varying levels of cyber capabilities in support of their strategic national objectives. The Russian 'New Generation Warfare' has evolved to the 'New-Type of War' applying operational art as a means to gain an asymmetric advantage over an enemy's technological advantage. Fundamental to gaining this advantage is the employment of cyberwarfare.

The Army's multi-domain battle concept outlines emerging requirements for the military to achieve effects in the contemporary operational environment against emerging near peer threats. Cyber capabilities are critical to enable operational commanders the opportunity to create temporary windows of advantage, shape the deep fight, control tempo of multi-domain operations, and arrange cyber effects in time and space to achieve strategic objectives. Both case studies, the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016, demonstrate cross domain synergy achieved with successful application of cyber electromagnetic activities (CEMA) to provide opportunities during multi-domain operations.

The significance of this research is that it contributes to an understanding of cyberwarfare as applied through the lens of operational art and multi-domain battle. The study provides a conceptual framework to assist in answering two key questions. First, how do military forces offensively and defensively employ cyber capabilities? Second, how can the US Army develop an operational approach to gain an advantage in the cyber domain and synergy across other domains to create windows of advantage?

Contents

Acknowledgement

I would like to thank Dr. Bruce Stanley for guiding me through the monograph process. I am definitely a better leader for the growth and knowledge gained throughout the year under your leadership and mentorship. I would also like to thank Colonel J. Scot Davis, who reviewed multiple drafts for me, and provided seminar nine with outstanding professional advice and discussion throughout the academic year. Last, but most importantly, I want to thank my wife Amber and our three daughters Lillian, Dieneka, and Margaret. Thank you for your patience and understanding. You allowed me to work long hours in the summer and fall so that I could complete this project as quickly and efficiently as possible. Thank you for your sacrifice, unconditional love and support throughout this year.

Acronyms

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
APT	Advanced Persistent Threats
CEMA	Cyberspace Electromagnetic Activities
CM	Combat Mission
COG	Center of Gravity
C2	Command and Control
COMINT	Communications Intelligence
DoD	Department of Defense
DDoS	Distributed Denial of Services
DODIN	Department of Defense Information Network
ELINT	Electronic Intelligence
EW	Electronic Warfare
FM	Field Manual
IMF	International Monetary Fund
IP	Information Packet
IPB	Intelligence Preparation of the Battlefield
JFC	Joint Force Commander
JOAC	Joint Operational Access Concept
JP	Joint Publication
MDMP	Military Decision Making Process
MILDEC	Military Deception
MISO	Military Information Support Operations
NATO	North Atlantic Treaty Organization
RC	Reflexive Control

SCADA	Supervisory Control and Data Acquisition
SG	Surface Search Radar (US Navy)
SCR	Signal Corps Radio
SLOC	Sea Lines of Communication

Introduction

> When the Nation calls upon the Army to fight and win its next war, the operational environment…will be defined by an enemy who will challenge our ability to maintain freedom of maneuver and superiority across the air, cyberspace, land maritime, and space domains and the electromagnetic spectrum…To counter our state-of-the-art communications network, they may hack in, disrupt, and deny our assurances through a well-organized group of experts hitting targets purposefully selected with intelligence and acting in accord with a larger maneuver plan—all executed from outside the area of operations.
>
> —General David G. Perkins, *Military Review*

Multi-Domain Battle is the Army's new concept for future warfare with lineage from the AirLand Battle concept of the 1980's. The Airland Battle concept began an open dialogue across the Army and is attributed as the genesis of FM 100-5, *Operations*.[1] The current operational environment and the emerging challenges of near peers and non-state actors have combined to create a challenge for the United States to gain and maintain the advantage across all three levels of war and across all domains. China, Russia, North Korea, and Iran have developed and implemented varying levels of cyber capabilities in support of their strategic national objectives.[2]

The Russians and Chinese have focused efforts over the last decade to increase their capability to offset US military strengths. The Russian 'New Generation Warfare' has evolved to the 'New-Type of War' concept. General-Lieutenant Andrey V. Kartapolov outlined the concept in 2015 as a means to gain an asymmetric advantage over an enemy's technological advantage.[3]

---

[1] GEN David G. Perkins, "Multi-Domain Battle: Driving Change to Win in the Future," *Military Review* (July-August 2017): 8.

[2] Jonathan Bott, "Outlining the Multi-Domain Battle Concept," June 8, 2017, accessed August 19, 2017, https://overthehorizonmdos.com/2017/06/08/outlining-the-multi-domain-operating-concept/.

[3] Andrey V. Kartapolov, "Lessons of Military Conflicts and Prospects for the Development of Resources and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts," *Vestnik Akademii Voennykh Nauk 2* (*Journal of the Academy of Military Science 2*) (2015): 35, quoted in Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* (July-August 2017): 39.

Fundamental to gaining this advantage is the employment of cyberwarfare and 'software effects.'[4]

The Army's multi-domain battle concept outlines emerging requirements for the military to achieve effects in the contemporary operational environment against emerging near peer threats. Cyberwarfare capabilities are a critical component to creating and exploiting temporary windows of advantage at the operational level.[5] Operational planners must employ operational art to arrange cyber effects in time and space to achieve strategic objectives against near peer threats, across all domains. Cyber capabilities are critical to warfare to allow operational level commanders the opportunity to shape the deep fight and control tempo of multi-domain, joint operations.

The significance of this research is that it contributes to an understanding of cyberwarfare as applied through the lens of operational art and its contribution to multi-domain battle. An effective operational approach will provide the operational commander the opportunity to create temporary windows of advantage by leveraging the cyber domain across other domains. The study provides a conceptual framework to assist in answering two key questions. First, how do military forces offensively and defensively employ cyber capabilities? Second, how can the US Army develop an operational approach to gain an advantage in the cyber domain and synergy across other domains to create windows of advantage?

These questions require a common understanding of several terms: cyberwarfare, operational art, tempo, cross-domain synergy, and multi-domain operations. Cyberwarfare is an "act of war that includes a wide range of activities using information systems as weapons against

---

[4] Kartapolov, "Lessons of Military Conflicts and Prospects for the Development of Resources and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts," 35, quoted in Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* (July-August 2017): 40.

[5] US Army Training and Doctrine Command, White Paper, "Multi-Domain Battle: Combined Arms for the 21st Century," February 24, 2017, accessed July 19, 2017, http://www.tradoc.army.mil/multidomainbattle/docs/MDB_WhitePaper.pdf.

an opposing force."[6] US Army Doctrinal Reference Publication (ADRP) 3-0 *Operations* defines operational art as the, "pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose."[7] Operational artists build campaigns through intermediate objectives across lines of operations over time. Army planners achieve strategic objectives through creating an operational approach that acts as the bridge between tactical actions and success, to strategic aims. Tempo is the, "relative speed and rhythm of military operations over time with respect to the enemy."[8] Additional attributes of tempo considered in this study will be the aspects of frequency, duration, sequencing, and opportunity.[9] The Multi-domain battle white paper refers to the recognized five domains of air, land, maritime, space, and cyberspace; in addition it refers to the electromagnetic spectrum, information environment, and cognitive dimension of warfare as contested areas.[10] Cross-domain synergy is "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others."[11] The joint force routinely employs air, land, maritime, space, and/or cyberspace capabilities to impact operational tempo and create multiple dilemmas for the enemy commander, thereby paralyzing

---

[6] Mike Chapple and David Seidl, *Cyberwarfare: Information Operations in a Connected World* (Burlington, MA: Jones and Bartlett Learning, 2015), 389, accessed August 19, 2017, https://books.google.com/books?id=EVwtBAAAQBAJ&printsec=frontcover&dq=cyberwarfare&hl=en&sa=X&ved=0ahUKEwi2u695uTVAhUp74MKHXYTDU0Q6AEITzAG#v=onepage&q=cyberwarfare%20defined&f=false.

[7] US Department of the Army, Army Doctrinal Reference Publication (ADRP) 3-0, *Operations* (Washington, DC: Government Printing Office, 2016), 2-1.

[8] Ibid., 2-7.

[9] Robert R. Leonhard, *Fighting by Minutes: Time and the Art of War* (Westport, CT: Praeger, 1994).

[10] US Army Training and Doctrine Command, "Multi-Domain Battle."

[11] US Department of Defense, *Joint Operational Access Concept (JOAC) Version 1.0* (Washington, DC: United States Department of Defense, 2012), Foreword, accessed August 19, 2017, https://www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf.

the enemy decision cycle.[12] Synergy is achieved with simultaneous action across multiple or all domains.[13]

This research relies on three hypotheses. First, when an operational approach arranges cyber capabilities across all domains it will create time and space allowing the operational level commander to shape the deep fight and control the tempo of joint operations. Second, when cyber capabilities are used across all domains they provide the operational commander time and space in the defense to expose and increase enemy vulnerability by forcing the enemy to concentrate forces.[14] Third, when cyber capabilities are employed in the offense across all domains the arrangement achieved will allow operational commanders the time, space and ability to seize, retain, and exploit the initiative, gaining the advantage against the threat. [15]

Eight research questions are used to gather evidence to test the three hypotheses. First, what are cyber capabilities in the defense? Second, what is the current US operational approach to the implementation of cyber capabilities at the operational level? Third, what are cyber capabilities in the offense? Fourth, what are examples of cross domain effects providing time, space, and operational advantage? Fifth, what can cyber do to integrate cross domain capabilities to buy time and space for the commander? Sixth, what are current enemy cyber capabilities and methods of employment at the operational level? Seventh, what are the contributions of cyber to

---

[12] US Department of Defense, *Joint Operational Access Concept (JOAC) Version 1.0*, ii.

[13] US Joint Staff Joint Force Development (J7)- Future Joint Force Development, *Cross-Domain Synergy in Joint Operations, Planner's Guide*, January 14, 2016, 1, accessed August 19, 2017, http://www.dtic.mil/doctrine/concepts/joint_concepts/cross_domain_planning_guide.pdf.

[14] A defensive task is a, "task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks." US Department of the Army, Army Doctrinal Reference Publication (ADRP) 3-0, *Operations* (Washington, DC: Government Printing Office, 2016), 3-4.

[15] The main purpose of the offense, "is to defeat, destroy, or neutralize the enemy force." US Department of the Army, Army Doctrinal Reference Publication (ADRP) 3-90, *Offense and Defense* (Washington, DC: Government Printing Office, 2012), 3-1.

the Deep Battle concept and reflexive control (RC)? Eighth, what critical capabilities across all domains are linked to cyber capabilities and critical vulnerabilities?

This research focused on only unclassified, publicly released information. The primary purpose of the analysis centered on the cyber domain and its ability to impact the land domain through cross-domain synergy and effects. The paper attempts to apply operational art in the context of the cyber domain to develop a multi-faceted operational approach to create an advantage for the operational level commander and staff. Two historical case studies are used to develop and inform the understanding of the cross-domain exponential advantage gained through exploitation and synergized effects of application of cyber capabilities across multiple domains. These case studies provide examples of how the application of cyber capabilities across multiple domains can create opportunities.

The study is organized into seven sections: the introduction, literature review, methodology, case studies, findings, analysis, and conclusion. The literature review builds a theoretical foundation of operational art, joint cyber capabilities, and cyberwarfare and how those capabilities are currently implemented across all domains. Next, the methodology provides a framework and approach to determine how cyber capabilities integrate across domains pointing to an operational approach to achieve synergy and desired effects. Next, the case studies will illuminate, through historical examples, how temporary windows of advantage in one domain have created exponential capability in other domains. The findings section will synthesize the case study findings within the theoretical framework. Finally, the conclusion draws from the findings to recommend an operational approach for the application of cyber capabilities across joint operations allowing the operational commander multi-domain windows of advantage.

Literature Review

The literature review provides a logical framework for the basis of this study. Once established, this framework provides the theoretical lenses and parameters for the discussion,

methodology and how the case studies will be viewed. First, operational art will be discussed within the evolution of the US doctrinal framework and prominent thinkers and Russian deep battle concept. Second, the two aforementioned operational art frameworks will be combined with current joint and Army cyberspace doctrine to provide a structured focused approach to assess the subsequent case studies and analyze potential multi-domain advantages to be gained through cyber capabilities. The case studies will include: the Russian conflicts with Ukraine and the WWII campaign for Guadalcanal.

US Operational Art

Operational art provides the bridge between tactical actions and strategic objectives. It involves a systematic and deliberate campaign planning process for major operations in a theater of war.[16] There are nuanced differences among joint and Army doctrine on the exact meaning of operational art since its emergence in the US Army in the 1980's. Joint Publication 3-0 *Joint Operations* includes the development of campaigns and operations by "integrating ends, ways and means…reach the desired military end state in support of national objectives."[17] Additionally, operational art incorporates operational design "the conception and construction of the framework that underpins a joint operation or campaign plan and its subsequent execution"[18] to provide linkage and an operational approach over time between the overall tasks, purposes and desired end state for a campaign. Joint Publication 5-0 *Joint Planning* defines in detail the purpose of operational art and operational design. There are thirteen elements of operational design that assist in visualizing the problem and developing an effective operational approach. The elements are; termination, military end state, objectives, effects, center of gravity, decisive

[16] John Andreas Olsen and Martin van Creveld, *The Evolution of Operational Art: From Napoleon to the Present* (Oxford: Oxford University Press, 2011), 1.

[17] US Department of Defense, (JP 3-0), *Joint Operations* (Washington, DC: United States Department of Defense, 2017), xii.

[18] Ibid., II-4.

points, lines of operations and lines of effort, direct and indirect approach, anticipation, operational reach, culmination, arranging operations, and forces and functions.[19]

US Army doctrine details operational art in ADRP 3-0 *Operations*. The Army released FM 100-5, *Operations* in 1982 when it previewed the AirLand Battle concept and the term has experienced multiple evolutions over the last thirty-five years. The emergence of operational art and AirLand Battle sought to synchronize efforts across all domains and warfighting functions to maximize capability in time and space and counter the Soviet threat at the time.[20] ADRP 3-0 defines operational art as the "pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose."[21] The Army includes ten elements of operational art: end state and conditions, centers of gravity, decisive points, lines of operations and lines of effort, basing, tempo, phasing and transitions, culmination, operational reach, and risk.[22] Five of the ten Army elements are common to the elements of operational design joint doctrine mentioned previously from JP 5-0.

In addition to doctrine, three prominent theorists and writers have informed this paper's definition of operational art. In his book, *Napoleon's Last Victory: 1809 and the Emergence of Modern War*, Robert Epstein defines operational campaigns as "characterized by symmetrical conscript armies organized into corps, maneuvered in a distributed fashion so that tactical engagements are sequenced and often simultaneous, command is decentralized, yet the commanders have a common understanding of operational methods. Victory is achieved by the

---

[19] US Department of Defense, (JP 5-0), *Joint Planning* (Washington, DC: United States Department of Defense, 2017), IV-19.

[20] Antulio J. Echevarria, "American Operational Art, 1917-2008," *The Evolution of Operational Art: From Napoleon to the Present*, ed. John Andreas Olsen and Martin van Creveld (New York: Oxford University Press, 2011), 155.

[21] US Army, ADRP 3-0, (2016), 2-1.

[22] Ibid., 2-4.

cumulative effects of tactical engagements and operational campaigns."[23] The advent of modern warfare saw the end to the possibility of one decisive battle. The commander and staff in modern war must understand and visualize the linkages between multiple battles or tactical actions and arrange them over time and space to achieve the overall end state and strategic objectives. The critical aspects from Epstein's definition are the cumulative effects and the plurality of the requirement of multiple engagements and campaigns. Operational art is founded on an operational approach that links multiple tactical actions into campaigns over time to achieve the objective.

The next critical thinker who greatly contributed to the overall understanding of operational art is Dr. James Schneider and his *Theoretical Paper No. Four, Vulcan's Anvil: The American Civil War and the Foundations of Operational Art*. Schneider defines operational art as "a unique style of military art, became the planning, execution and sustainment of temporally and spatially distributed maneuvers and battles, all viewed as one organic whole."[24] According to Schneider, operational art is characterized by eight attributes: distributed operations, distributed campaigns, continuous logistics, instantaneous command and control, operationally durable formations, operational vision, distributed enemy, and distributed deployment.[25] Schneider's definition of operational art demonstrates the foundation of the understanding of both time and space separating maneuvers and the linkage to an overall whole or goal. Additionally, the attributes he defines link to our current, Army and Joint doctrines' elements of operational art and design. All of the elements of operational art and design are interrelated variables that must be considered holistically to determine the most effective operational approach to solve a problem.

---

[23] Robert M. Epstein, *Napoleon's Last Victory and the Emergence of Modern War* (Lawrence: University Press of Kansas, 1994), 6.

[24] James, J. Schneider, *Vulcan's Anvil: The American Civil War and the Foundations of Operational Art, Theoretical Paper No. Four* (Fort Leavenworth, KS: School of Advanced Military Studies, Command and General Staff College, 1992), 28.

[25] Ibid., 35-58.

The next aspect of operational art critical to this study is the combination of the theory of operational art and systems theory from Shimon Naveh. Within the complexity of the contemporary operational environment it is critical to account for the challenges within the operational level of war. Three critical concepts taken from Naveh are the requirements for operational art, the concept of operational shock, and operational vulnerability. Naveh describes nine requirements for operational art or an operational level plan: 1) reflect the cognitive tension between the strategic and tactical levels of war; 2) based on productive maneuver reflecting the link from tactical action and strategic aim; 3) must be synergetic (the sum of the whole is greater than the individual parts) and integrate forces in time and space that are geographically and spatially separate; 4) aim at the disruption of the opponent's system; 5) account for chaos within the conflict of systems on systems; 6) non-linear in nature, hierarchical and express across the depth of the operational environment; 7) reflect the deliberate interaction between maneuver and attrition or erosion of the opponent; 8) although reliant on the strategic level for aims, restrictions and resources, it is still an independent entity; 9) must be related to a broad and universal theory.[26]

Naveh continues to develop the understanding of operational art with his discussion of operational shock. Operational shock "delineates in practical terms a consequential state of a fighting system which can no longer accomplish its aims."[27] Naveh's systems approach to operational art provides insight to developing a practical operational approach to link tactical actions in time and space to achieve strategic objectives and aims. As a system, the military interacts within multiple systems targeting the enemy systems to achieve the effect of shock or

[26] Shimon Naveh, *The Cummings Center Series*, vol. 7, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (London: Frank Cass, 1997), 13-14.

[27] Ibid., 16.

paralysis, thereby preventing the enemy from achieving their aim and allowing our victory and subsequent success operationally and strategically.

Naveh further outlines two potential weaknesses within a military system vulnerable to shock, which will assist in protecting our critical vulnerabilities as well as identifying and attacking the enemy's. The two potential weaknesses are: 1) absolute dominance of the aim; 2) deep structure and hierarchic logic of action.[28] In keeping these weaknesses in mind Naveh outlines three methods for exploiting the system's structure and weaknesses. First is division and fragmentation in depth, both horizontally and vertically.[29] This multi-dimensional action will disrupt the synergy of the enemy system across the breadth of the formation and in-depth at echelon disrupting the ability of the enemy to command, control, communicate, and synchronize. The enemy system will be broken down into individual parts thereby creating shock. Second, the attacks on the enemy must achieve simultaneity throughout the depth of the enemy formation with multiple concurrent and synchronized operations. Finally, shock can be created with attacks on the center of gravity.[30] There are three critical components to identify: 1) the exact points of strength and weakness in the opposing system; 2) the deliberate creation of operational vulnerabilities in it; 3) the exploitation of vulnerabilities through maneuver.[31]

Russian Operational Art

Russian operational art began under Aleksandr Svechin during the 1920's. He defined operational art as the conceptual linkage between strategy and tactics, where commanders link

---

[28] Naveh, *The Cummings Center Series*, vol. 7, *In Pursuit of Military Excellence: The Evolution of Operational Theory*, 16-17.

[29] Ibid., 17.

[30] Ibid., 18.

[31] Ibid., 19.

successes tactically with operational bounds to strategic objectives.[32] Svechin proposed a strategy of attrition as an option outside of destruction in a decisive battle. The goal of attrition is to gradually deplete the enemy's capability to wage war over a successive series of tactical engagements. "The operations of a strategy of attrition are not so much direct stages toward the achievement of an ultimate goal as they are stages in the deployment of material superiority, which would ultimately deprive the enemy of means for successful resistance."[33]

M. N. Tukhachevsky has also been credited with the development of Soviet operational art and the concept of mechanization, militarization of the Soviet economy, deep battle and its transformation into deep operations theory focusing on the annihilation of the enemy through the depth of his defenses.[34] He first detailed his understanding of the modernization of war and operational level of warfare in a 1926 article.

> Modern tactics are characterized primarily by organization of battle, presuming coordination of various branches of troops. Modern strategy embraces its former meaning: that is the 'tactics of a theatre of military operations'. However, this definition is complicated by the fact that strategy not only prepares for battle, but also participates in and influences the course of battle. Modern operations involve the concentration of forces necessary to deliver a strike, and the infliction of continual and uninterrupted blows of these forces against the enemy throughout an extremely deep area. The nature of modern weapons and modern battle is such that it is impossible to destroy the enemy's manpower by one blow in a one-day battle. Battle in modern operations stretches out into a series of battles not only along the front but also in depth until that time when either the enemy has been struck by a final annihilating blow or the offensive forces are exhausted. In that regard, modern tactics of a theater of military operations are tremendously more complex than those of Napoleon. And they are made even more complex by the

---

[32] Jacob W. Kipp, "The Tsarist and Soviet Operational Art, 1853-1991," in *The Evolution of Operational Art: From Napoleon to the Present*, ed. John Andreas Olsen and Martin van Creveld (New York: Oxford University Press, 201), 65.

[33] Aleksandr Svechin, *Strategy*, ed. Kent D. Lee (Minneapolis, MN: East View Publications, 1992), 247.

[34] Kipp, "The Tsarist and Soviet Operational Art, 1853-1991," 70-71.

inescapable condition mentioned above that the strategic commander cannot personally organize combat.[35]

Tukhachevsky understood the requirements for an operational level of war to provide the linkage between strategy and tactical actions across the battlefield and throughout the entire depth of an enemy. He also postulated the importance of the critical factors of depth, continuity, synergism and wholeness and developed an understanding of operational shock (*udar*) and impacts in the enemy as a system.[36] The overarching goal is to create an operational approach that will achieve simultaneous paralysis of the entire depth and breadth of the enemy formation through operational maneuver. This paralysis will neutralize the opponent's system and subcomponents creating the opportunity for annihilation and victory and achieving the strategic goal. Isserson further developed the concept and provided models for the operational formations that would achieve a deep breakthrough. A hallmark of his concept is developing 'depth-to-depth blows' and 'operational simultaneity.'[37]

Current Russian strategy has continued to modernize the deep battle concept with the two critical aspects of 'new-type warfare' and reflexive control. The Russians have developed New-type warfare in an effort to gain asymmetric advantage against an opponent's technological advantage, specifically that of the United States.[38] General-Lieutenant Andrey Kartapolov in 2015 described the theory and key components. Kartapolov postulates that new-type warfare

---

[35] M. N. Tukhachevskii, 'Voina' (War), 1926, in A.B. Kadishev (ed.), *Voprosy strategii I operativnogo iskusstva v sovetkikh voennykh trudakh 1917-1940* gg. (Questions of Strategy and Operational Art in Soviet Military Works 1917-1940) (Moscow, 1965), pp 104-5 quoted in Shimon Naveh, *The Cummings Center Series*, vol. 7, *In Pursuit of Military Excellence: the Evolution of Operational Theory* (London: Frank Cass, 1997), 10-11.

[36] Naveh, *The Cummings Center Series*, vol. 7, *In Pursuit of Military Excellence: The Evolution of Operational Theory*, 11.

[37] Georgii Samoilovich Isserson, *The Evolution of Operational Art*, trans. by Bruce W. Menning (Fort Leavenworth, KS: Combat Studies Institute Press, 2013), 67-69.

[38] Kartapolov, "Lessons of Military Conflicts and Prospects for the Development of Resources and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts," 39.

involves 80-90 percent propaganda and 10-20 percent violence.[39] He provided a graphic that outlines the phases of New-Type warfare (see Appendix 1, Figure 1). Deep battle resonates throughout and it expounds the development of Russian operations across domains to shape operations prior to conflict using "hybrid methods" across multiple domains to create windows of advantage.

The second modern Russian theoretical concept is reflexive control. Reflexive control is applied as a means to interfere and manipulate an opponent's decision-making cycle. It can target human decision making and organizational decision-making systems and processes. Reflexive control can also be applied through automated systems and digital mission command architecture. Reflexive control is "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[40] One of the goals of reflexive control is the temporary slowdown of the adversary's tempo and operational level decision making process.[41] This adjustment in tempo creates windows of opportunity for Russian exploitation of changes in tempo and potential opponent decisions that shape the operational level forces into the overall Russian operational design and approach.

A significant aspect of RC is the targeting of technology as well. The goal is to use RC control as a shaping operation to disrupt the opponent's understanding of the operational environment. Through manipulation of reconnaissance assets, satellites, weapons guidance

---

[39] Kartapolov, "Lessons of Military Conflicts and Prospects for the Development of Resources and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts," 40.

[40] Timothy L. Thomas, *Kremlin Kontrol: Russia's Political-Military Reality* (Fort Leavenworth, KS: Foreign Military Studies Office, 2017), 176.

[41] V.B Veprentsev, A.V. Manoylo, A.I. Petrenko, and D.B. Frolov, Operations in Information-Psychological War: Short Encyclopedic Dictionary, Moscow: Hotline—Telecom, (2011), 446-448 quoted in Timothy L. Thomas, *Kremlin Kontrol: Russia's Political-Military Reality* (Fort Leavenworth, KS: Foreign Military Studies Office, 2017), 177.

systems and associated technology and systems used by the opponent, the Russians use RC to shape opponent understanding, feint direction of attacks, and manipulate portions of the mission command architecture.[42] RC is part of the Russian targeting methodology and process to identify weak links and means to exploit. The interference at a minimum aims to achieve temporary paralysis of the opponent's decision-making process and operational tempo.[43]

Another critical aspect of reflexive control is the concept of complex or double-track control. Critical and corresponding to control of the enemy is the ability to exercise appropriate mission command over friendly forces. Reflexive control creates windows of opportunity for exploitation. In order to exploit the opportunity, Russian friendly units must have a plan in place to exploit the opportunity and gain the initiative at the tactical, operational and strategic levels. Reflexive control requires synchronization and has a spatial-temporal aspect.[44] Appendix 1, figures 2 and 3 are visual depictions of the planning methodology linking the Russian decision-making process to reflexive control of the enemy, the information packet (IP), and the combat mission (CM) of Russian elements seeking to exploit the process.

US Joint and Army Cyber Doctrine

Critical to the understanding of US cyber capabilities is an understanding of the Department of Defense (DoD) cyber strategy as well as joint and army doctrine for cyberspace operations, and joint doctrine on cross domain synergy. The focus of this section on cyberspace is not to provide an exhaustive list of the history of cyberspace, but to introduce the current doctrine for employment in order to inform the implementation and understanding of cross domain

---

[42] S. Leonenko, "On Reflexive Control of the Enemy," *Armeyskiy Sbornik (Army Digest)*, 8 (1995): 28, quoted in Timothy L. Thomas, *Kremlin Kontrol: Russia's Political-Military Reality*, (Foreign Military Studies Office, Fort Leavenworth, KS, 2017), 179.

[43] V.L. Makhnin, "Reflexive Processes in Military Art: The Historico-Gnoseological Aspect," *Voennaya Mysl' (Military Thought)*, 1 (2013): 40 quoted in Timothy L. Thomas, *Kremlin Kontrol: Russia's Political-Military Reality*, (Fort Leavenworth, KS: Foreign Military Studies Office, 2017), 188.

[44] Thomas, *Kremlin Kontrol: Russia's Political-Military Reality*, 194.

advantage opportunities as applied in the case study methodology. Additionally, it is important to have a foundational knowledge of those cyberspace electromagnetic activities (CEMA) to implement as part of an operational approach and to counter the Russian operational methodology for employment.

The Department of Defense published *The DoD Cyber Strategy* in 2015. It outlines the major considerations and priorities for US cyberspace operations. There are three primary cyber missions, two defensive and one offensive in nature: "1) DoD must defend its own networks, systems, and information; 2) DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence; 3) if directed by the President or Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans."[45] The primary mission consideration for this study will be the third mission of integration of cyber capabilities to support military operations across the DoD and implied across multiple or all domains.

In addition to the three missions, the DoD strategy also identifies five strategic goals: 1) Build and maintain ready forces and capabilities to conduct cyberspace operations; 2) Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions; 3) Be prepared to defend the US homeland and US vital interests from disruptive or destructive cyberattacks of significant consequences; 4) Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment in all stages; 5) Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.[46] The strategic goals most relevant to an operational level impact and this study are goals two and four. The DoD Information Network (DODIN) is

[45] US Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Government Printing Office, 2015), 4-5.

[46] Ibid., 7-8.

employed at all levels of war and will be targeted specifically at the operational level to impact the decision-making process, shape US actions through reflexive control, technological interference, and manipulation of mission command architecture and systems. Cyber applications will also be used both offensively and defensively to facilitate control of conflict escalation and to shape the operational environment throughout military operations across all domains.

Joint Publication 3-12 (R) *Cyberspace Operations* describes in detail the cyberspace environment, cyberspace operations, and the implications for the joint planning and operations process including the planning, preparation, execution and assessment. Cyberspace operations "are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[47] Cyberspace is unique in the aspect of being one of the five domains (air, land, maritime, space and cyber) but also operating across three cyberspace layers (physical network, logical network, cyber-persona) while providing critical linkages across all physical domains and across all six functions of joint operations (command and control, intelligence, fires, movement and maneuver, sustainment, protection).[48] Cyberspace operations allow the commander to retain freedom of maneuver across cyberspace, accomplish the Joint Force Commander's (JFC) objectives, deny freedom of action to the enemy, and enable other operations across the other physical domains.[49] As the US military becomes more dependent on cyberspace for communication, planning, mission command, and sustainment we will become more susceptible to cyber attack and targeting from adversaries. The physical domains have become dependent on the cyber domain as it relates to specific functions and tempo within the physical operating environment.

---

[47] US Department of Defense, Joint Staff, Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 2013), v.

[48] Ibid., v-viii.

[49] Ibid., I-6.

There are three primary types of cyberspace operations, offensive, defensive and DODIN which are intent based. The types of cyber operations will determine planning priorities and also reveal potential vulnerabilities of the cyber domain during military operations. Offensive operations "are cyber operations intended to project power by the application of forces in and through cyberspace."[50] Cyber operations are interwoven within information operations to include military information support operations (MISO) and military deception (MILDEC). Defensive cyberspace operations are "intended to defend DoD or other friendly cyberspace…they are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[51] The final aspect relevant to this study are DODIN operations. DODIN operations are "actions taken to design, build, configure, secure, operate, maintain and sustain DoD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation."[52]

Additionally, cyberspace operations are broken down into cyberspace actions. These actions are tied to achieving effects and can assist in understanding at the operational level as cyberspace operations tie into the joint planning and targeting process. There are four cyberspace actions available to the joint commander: 1) cyberspace defense; 2) cyberspace intelligence, surveillance, and reconnaissance (ISR); 3) cyberspace operational preparation of the environment; 4) Cyberspace attack.[53] Cyberspace attack has ramification both in the cyber and physical domains as it can achieve the effects of deny or manipulate. Deny is directly related to time and therefore can impact an opponent's tempo with respect to opportunities for decisions, sequencing and frequency. To deny is to "degrade, disrupt, or destroy access to, operation of, or

[50] US Joint Staff, JP 3-12 (R), (2013), II-2.

[51] Ibid., II-2.

[52] Ibid., II-3.

[53] Ibid., II-4-II-5.

availability of a target by a specified level for a specified time…prevents adversary use of resources."[54] To manipulate is to "control or change the adversary's information, information systems, and/or networks in a manner that supports commander's objectives."[55]

Field Manual 3-12 *Cyberspace and Electronic Warfare Operations* was published in April 2017 to guide US Army cyber operations. The manual is nested with the joint and DoD documents previously addressed. The major significance for this study is the inclusion of cyber operations in planning considerations within the military decision making process (MDMP) and targeting process. The goal of the application of cyber capabilities is to synchronize simultaneous and complementary effects across domains to gain a position of advantage. JP 3-0 defines joint targeting as the "process of selecting and prioritizing targets and matching the appropriate response to them, taking account of command objectives, operational requirements, and capabilities."[56] Due to the complexity of cyberspace operations and the multiple layers of the domain a significant effort must be placed throughout the planning process, specifically Intelligence Preparation of the Battlefield (IPB).[57] Additionally, the cyber domain involves aspects across multiple domains and also the functional commands requiring additional coordination to acquire the appropriate command level authority to authorize target execution and maintain synchronization at the operational level with operations to achieve the desired effect. Finally, aspects of cyber capabilities exist in the physical domains and can be targeted by other assets. The targeting boards at the various Army and joint commands must be involved to assist in prioritization of assets used to strike as well the priority of the opponent's capabilities to target.

---

[54] US Joint Staff, JP 3-12 (R), (2013), II-5.

[55] Ibid.

[56] US Joint Staff, JP 3-0, (2017), III-26.

[57] US Department of the Army, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: Government Printing Office, 2017), 3-22.

The Army targeting methodology follows the four-step construct of decide, detect, deliver and assess. FM 3-12 applies the targeting process to CEMA specifically and outlines key considerations for each step of the process. Decide and detect are two critical steps in the targeting process based on the requirements for integration in the approval and prioritization process and the intel and information collection plan. The first step, decide, requires a deliberate plan to identify enemy capabilities based on the potential anonymity cyberspace provides and which domain and weapon system will best achieve the desired effects to create cross domain synergy.[58] The second step, detect, is also tied to the information collection plan. Situational understanding is critical and is attained through "situational data as geospatial location, signal strength, system type, and frequency of target to focus effects on the intended target."[59]Additionally, targets must be developed through the collection plan, vetted, validated and approved for prosecution as part of the target nomination and collection plan processes. The third step is deliver. Delivery must be synchronized in time and space to achieve the operational commander's purpose. Additionally, it will most likely need to be synchronized to achieve synergy with operational maneuver in the physical domains. The multiple levels of the approval process require early target approval to allow for application in a timely manner at the operational level. The final step in the targeting process is assess. Intelligence and maneuver assets can be tied to the assessment of cyber actions to determine effectiveness and whether it requires reengagement. However, effects produced in cyberspace are not always physically visible or apparent, especially to the echelon requesting the effect.[60] The appropriate level must be tied into the operational level for feedback and effects. Additional considerations must be made for enemy capabilities to detect and mitigate the cyber effects and impacts on commander's decisions for

[58] US Army, FM 3-12, (2017), 3-23.

[59] Ibid.

[60] Ibid.

additional assets to create the desired window of opportunity within the cyber domains or impacts on desired cross domain effects and synergy.

The final doctrinal concept for review is the idea of cross domain synergy. The joint document *Cross-Domain Synergy in Joint Operations Planner's Guide* details the concept in relation to the joint planning process (JPP). The overall purpose is to gain efficiency and effectiveness across all domains and their capabilities to assist the joint force in accomplishing the mission.[61] The focus of the document is on planning but the concept also applies to the execution of operations as well. Cross domain synergy is "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others."[62] The joint force routinely employs all domain (air, land, maritime, space, and cyberspace) capabilities to overwhelm an adversary's ability to decide and act.[63] Although the Planner's Guide focuses on the planning process, inherently involved as well is the execution and feedback elements of the operations process.

The ability to operate in multiple domains also allows the operational commander multiple opportunities and options to apply force across all domains against enemy weaknesses,[64] thereby creating options for the friendly force and multiple dilemmas for the enemy. The cross-domain synergy gained will impact the enemy's decision-making process and systems, and have implications on the enemy's ability to understand, visualize, describe the operational environment and take appropriate actions. Cross domain synergy will inherently help create paralysis and

---

[61] US Joint Staff Joint Force Development (J7)- Future Joint Force Development, *Cross-Domain Synergy in Joint Operations, Planner's Guide,* Preface.

[62] US Department of Defense, *Joint Operational Access Concept (JOAC) Version 1.0*, Foreword.

[63] Ibid., ii.

[64] US Joint Staff, *Cross-Domain Synergy in Joint Operations, Planner's Guide,* 5.

shock in the enemy system and windows of opportunity for the force to gain and maintain the operational advantage.

Methodology

This study employs the structured focus approach of multiple case studies. First, it is structured in that the same focused research questions are asked of each case study to guide and standardize collection, facilitate systematic comparison, and aid in analysis and findings.[65] Second, the study is focused because it will only deal with certain aspects of the two historical cases examined.[66] The overall desired end state is to determine aspects, methods and advantages gained through application of cross domain synergy to determine potential applications for the cyber domain to gain advantage across multiple domains. The elements of operational design and art from joint and Army doctrine, along with the additional operational art aspects from theory will be combined with aspects of Russian deep battle and reflexive control to provide an analysis tool for the two case studies involved. The structured focus methodology provides a way to assess the evidence of the case studies and determine aspects of cross domain synergy and applications to the future use of cyber capabilities.[67]

The critical factors provided a method of analysis of the two case studies to determine how advantages in one or more domains can impact other domains and overall synergy. The overall analysis will provide insight into how cyberspace capabilities within the cyber domain can provide temporary windows of advantage within other domains to create opportunities for the operational commander to accomplish the mission.

---

[65] Alexander L. George, *Case Studies and Theory Development in the Social Sciences*, Besia Studies in International Security (Cambridge, MA: MIT Press, 2005), 67.

[66] Ibid., 67.

[67] Ibid.

The significance of this research is that it contributes to the understanding of cyberwarfare as applied through the lens of operational art and its application to multi-domain battle. An effective operational approach will provide the operational commander the opportunity to create temporary windows of advantage by leveraging the cyber domain across other domains. The study provides a conceptual framework to assist in answering two key questions. First, how do military forces offensively and defensively deploy cyber capabilities? Second, how can the US Army develop an operational approach to gain an advantage in the cyber domain and synergy across other domains to create windows of advantage?

Eight research questions are used to gather evidence to test the three hypotheses. First, what are cyber capabilities in the defense? Second, what is the current US operational approach to the implementation of cyber capabilities at the operational level? Third, what are cyber capabilities in the offense? Fourth, what are examples of cross domain effects providing time, space, and operational advantage? Fifth, what can cyber do to integrate cross domain capabilities to buy time and space for the commander? Sixth, what are current enemy cyber capabilities and methods of employment at the operational level? Seventh, what are the contributions of cyber to the Deep Battle concept and reflexive control? Eighth, what critical capabilities across all domains are linked to cyber capabilities and critical vulnerabilities?

Two case studies will be used throughout this project and will be analyzed using the same aspects above. The two case studies will be: the Guadalcanal campaign 1942-1943 and Russian operations in Ukraine 2013-2016. The first historical case study will provide a foundation for cross-domain advantage and analysis. The second case study will carry those lessons forward and allow for detailed analysis of the Russian operational art concept of deep battle and modern application combined with new-type warfare and reflexive control.

The use of primary and secondary sources provided the data for the study. The historical case study of Guadalcanal provided analysis of the elements of operational art. Additionally, it provided examples of cross-domain advantage and synergy primarily across the land, air, and

maritime domains and electronic warfare (CEMA). The two case studies provide analysis of the research questions and modern examples of a near peer threat gaining multi-domain advantage using cyber capabilities.

The structured focused approach applied to these case studies will facilitate the objectives of this monograph and guide the evaluation of the three foundational hypotheses and eight research questions. Ultimately, the analysis will lead to an assessment of the application of operational art in multi-domain battle across the two cases to inform lessons for application of cyber capabilities to achieve cross domain synergy on the modern battlefield against a capable enemy. The next section will further analyze the case studies against the research questions to determine applicable lessons and analysis for developing an effective operational approach to apply cyber domain at the operational level.

Case Studies

Case study analysis assists us to analyze specific cases and determine relevant variables focused on a structured comparison to continue to refine concepts.[68] A total of two case studies will be used throughout this project and will be analyzed using the same aspects. The two case studies will be: the Guadalcanal 1942-1943 and Russia in Ukraine 2013-2016. The case studies will be developed and analyzed with a structured focus comparison of the established eight research questions. This analysis will lend to the refinement and clarification of multi-domain battle and the implications of the cyber domain across the other four domains.

Guadalcanal 1942-1943

Guadalcanal marked a more than ten-month campaign by US combined, joint forces to transition from the strategic and operational defense to the strategic and operational offense in the Pacific during World War II. In order to fully understand the case study, an understanding of the

[68] David Collier, "Comparative Historical Analysis: Where Do We Stand?" *American Political Science Association: Comparative Politics Newsletter*, 10 (Winter 1999): 1-6.

strategic context is necessary. The Battle of the Coral Sea, 7-8 May 1942 dealt a significant blow to the Japanese naval fleet, especially with the loss of four carriers with 250 aircraft and many highly trained aircrews.[69] The Battle of Midway 4-7 June 1942 marked another US victory and created a turning point ending the Japanese strategic offensive which originally intended to create the conditions through the offense to force US negotiations.[70]

United States and allied leadership began to see an opportunity to transition to the offense in the Pacific. The transition was critical to ensure the sea lines of communication (SLOC) to Australia, New Zealand, and New Guinea remained open. Additionally, the United States was supplying arms, equipment and advisors to China to keep them in the fight and maintain a force to fix Japanese Army capabilities on mainland Asia. The Japanese were attacking in Burma and extending their reach in the Pacific to sever the lines of supply to the Chinese. Both US and Japanese forces were at the limits of their operational reach. Subsequently this strategic context put the two belligerents on a collision course in the Solomon Islands and Guadalcanal, specifically.[71]

Joint operations during the Guadalcanal campaign included multi-domain aspects across four domains; air, sea, land, and electronic warfare/intelligence. The electronic warfare/intelligence (EW/intel) domain most closely resembles the aspects of cyber today and will be used to offer lessons applicable to cyber domain capabilities. Further analysis will also be completed to garner potential lessons from cross domain synergy achieved through impacts of actions from one domain to another.

---

[69] Richard B. Frank, *Guadalcanal: The Definitive Account of the Landmark Battle* (New York: Penguin, 1992, 1990), 24-25.

[70] Ibid., 25.

[71] William H. Bartsch, *Williams-Ford Texas A&M University Military History Series*, vol. 147, *Victory Fever On Guadalcanal: Japan's First Land Defeat of World War II* (College Station: Texas A&M University Press, 2014), 6-7.

The first research question is what are cyber capabilities in the defense? Electronic warfare capabilities were still in their infancy at the outset of World War II. Throughout the campaign for Guadalcanal, five major EW/intel capabilities assisted in gaining cross-domain advantage in the defense. The assets included coast watchers, local scouts, radars, the naval SG radar, and radio crypto-analyst. Assets in the air domain included the SCR-270 air warning radar delivered by the *Burrows* on 29 August and the coast watcher assets. Coast watchers were located on the islands of Bougainville and New Georgia. The coast watchers reported via radio any Japanese aircraft movement Southeast from Rabaul to Guadalcanal. The SCR-270 radar had a range of up to 130 miles and provided 35-40 minutes early warning of Japanese aircraft.[72] In the land domain, the local scouts operated under Captain Clemens to provide early warning of Japanese ground movements and offensive operations against Henderson Airfield. They greatly enhanced First Marine Division commander, Major General Vandergrift's ability to effectively use combat power available to seize and defend key terrain to deny the Japanese Army the ability to regain the airfield or affect air operations, airfield maintenance, and expansion.

The naval component was critical to operations to maintain the SLOC and supply to the Marines and pilots on Henderson Airfield. The SG radar proved critical in the naval fight on 13-14 November and achieved effects that prevented Japanese resupply operations while maintaining the SLOC to Guadalcanal. The SG radar had a range of 15 miles with a range accuracy of ± 100 yards and azimuth accuracy: ± 2°.[73] Rear Admiral Willis Lee expertly used the system on his flagship enabling Task Force 64 to identify the Japanese Tokyo Express run to reinforce and

---

[72] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 207.

[73] The Navy Department Library, Naval History and Heritage Command, U.S. Radar Operational Characteristics of Radar Classified by Tactical Application, FTP 217, prepared by Authority of the Joint Chiefs of Staff, by the Radar Research and Development Sub-Committee of the Joint Committee on New Weapons and Equipment, 1 August 1943, accessed October 27, 2017, https://www.history.navy.mil /research/ library/online-reading-room/title-list-alphabetically/u/operational-characteristics-of-radar-classified-by-tactical-application.html#sss.

resupply Japanese Army elements in the naval battle for Guadalcanal 13-14 November.[74] Lee not only denied Japanese naval efforts the ability to reinforce and resupply, but he also successfully screened and protected US naval efforts to assist the struggling First Marine Division on the island. In spite of heavy American naval losses, the delay allowed a transition to the air domain creating a window of opportunity for the Cactus Air Force to attack the remaining ships as they withdrew back to the Northeast toward Rabaul.

The final invaluable EW/intel asset used to great effect during the Guadalcanal campaign were the radio crypto-analysts. Crypto-analyst were able to intercept and decrypt a critical message on 8 November when Admiral Yamamato issued his orders for the November attack to reinforce and resupply Japanese Army elements on Guadalcanal. The analysts confirmed the Z-day for the operation for the 13th of November.[75] This valuable intelligence enabled Admiral Halsey to adequately plan and prioritize efforts for the defense of Guadalcanal as well as enabled naval and air efforts to focus capabilities for the intercept. The information proved invaluable for Admiral Lee in the naval battle for Guadalcanal 13-15 November which prevented Japanese naval reinforcement. The Japanese destroyer losses during that battle forced a transition to improvised methods of resupply with fifty gallon drums and submarines further affecting the land domain. The subsequent efforts continued to fail and the Japanese Army elements on the island operated near the edge of culmination and starvation.[76]

The second question is what is current US operational approach to the implementation of cyber capabilities at the operational level? The literature review section addressed current US cyber doctrine and theory for application. The primary focus on existing literature is at the strategic level and most recently at the tactical level with the publication of Field Manual 3-12,

---

[74] Robert Edward Lee, *Victory at Guadalcanal* (Novato, CA: Presidio Press, 1981), 253.

[75] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 426.

[76] Charles W. Koburger, *Pacific Turning Point: The Solomons Campaign, 1942-1943* (Westport, CT: Praeger, 1995), 118.

Cyberspace and Electronic Warfare Operations in April 2017. In order to adapt this question to the specific case studies, this study will address the operational approach for the implementation of electronic warfare at the operational level during the Guadalcanal campaign 1942-43.

The United States' focus for the application of EW spread across all three echelons: strategic, operational, and tactical. Prior to World War II the American intelligence community had broken the Japanese diplomatic code which used the Purple cypher machine.[77] Through the use of code breaking, also known as "Ultra," the joint forces were able to disrupt, delay, and prevent Japanese attempts to resupply and reinforce throughout the Solomon Islands.[78] Strategic and operational emphasis in the South Pacific was placed on radio intercepts, translation, and triangulation. It was far from an exact science. However, through atmospherics, location of the transmissions and volume of traffic, the radio traffic could be translated, decoded, and compared to determine Japanese plans for movement, resupply, and specific command structure for operations.[79]

The second aspect of EW is the ground based airborne radar. Following the Marine landing and securing of Henderson Airfield on 7-9 August 1942 the airfield was expanded to receive aircraft. The airfield was completed on 18 August. [80] The first SCR-270 reached the island on 20 September and was followed by two SCR-268's.[81] The SCR-270 enabled the operators to identify number and type of aircraft out to 200km. The SCR-268 allowed the operators to relay to the aircrews overhead the altitude of the enemy planes, greatly reducing the

---

[77] Frederik Nebeker, *Dawn of the Electronic Age: Electrical Technologies in the Shaping of the Modern World, 1914 to 1945* (Piscataway, NJ: IEEE, 2009), 404.

[78] Ibid.

[79] Rodney Carlisle, *Encyclopedia of Intelligence and Counterintelligence* (London, England: Routledge, 2015), 721-724, accessed October 31, 2017, http://ebookcentral.proquest.com/lib/columbia/detail.action?docid=2005326.

[80] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 127.

[81] Louis Brown, *A Radar History of World War II: Technical and Military Imperatives* (Bristol: Institute of Physics Pub., 1999), 249.

demands on the pilots, planes, and fuel.[82] This tactical success enabled the operational level commanders to mitigate risk as well as prioritize the flow of supplies (especially fuel, planes, and pilots) during the tenuous period from August to November of 1942.

The final aspect of operational implementation of EW was the employment of naval radars. Perhaps the greatest leadership failures at Guadalcanal revolved around the Navy's lack of understanding of the use of shipborne radar systems and the tactics to properly employ the systems with a mixed fleet of radar equipped ships at night. Five major surface engagements were fought in the vicinity of Guadalcanal and two carrier battles were fought just to the northeast. The Battle of Cape Esperance demonstrated a lack of understanding of new technologies based on both a quick timeline to development and secrecy surrounding the technology. Due in large part to the lack of understanding of the capabilities and improvements of the SG radars, Rear Admiral Scott did not switch his flagship to a light cruiser equipped with the SG radar.[83] Rear Amiral Scott was able to achieve effects against the superior night trained Japanese, but with significant US losses.

The naval battles of Guadalcanal 13-15 November taught additional lessons on the use of radars. The Japanese continued to deal heavy losses to the US Navy. Both key leaders, Admirals Callaghan and Scott chose flagships which were not outfitted with SG radar and both leaders were lost in the fight. Rear Admiral Lee provides a stark contrast to the previous naval failures. On the night of 14 November, he led a group of two battleships and four destroyers hastily put together. Lee faced off against a Japanese task force of a battleship, four cruisers, eighteen destroyers, and four transports.[84] Lee used the *Washington* as his flagship because it had SG radar capabilities and he knew how to use it. The US naval task force sank a destroyer and a battleship.

---

[82] Ibid., 250.

[83] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 294.

[84] Brown, *A Radar History of World War II: Technical and Military Imperatives*, 256-258.

[84] Ibid., 250.

The US successes delayed the Japanese transports forcing the Japanese commander to run them aground. All were lost the following day from air attacks.[85]

The third research question is what are the cyber capabilities in the offense? EW provided three major contributions to offensive operations. First, the radar systems provided early warning, in conjunction with coast watchers, of pending Japanese air attacks. The early warning provided for defense of Henderson Airfield, but assisted the Cactus Air Force offensively as well. The 40-45 minutes warning provided by the SCR-270 and SCR-268 gave adequate time for the pilots to get their aircraft to adequate altitude to contest the bombers and the zeros. Second, the discovery of a Japanese radar system on Guadalcanal by the Marines triggered an electronic intelligence (ELINT) requirement. The first B-17 ELINT missions began flying at the end of October to identify Japanese radar sets for future targeting.[86] The ELINT effort would become a shaping operation for future island hopping to establish the conditions for amphibious landings. Finally, communications intelligence (COMINT) provided early warning of the major Japanese reinforcement planned for 13 November.[87] The six days early warning gave both naval and air planners and leaders much needed time and focused intelligence to plan, prepare, and equip for the pending fight lending to the success of the naval and air battles 13-15 November 1942.

The fourth question is what are examples of cross domain effects providing time, space and operational advantage? Cross-domain synergy is "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others."[88] Multi-domain battle allows

> US forces to outmaneuver adversaries physically, virtually, and cognitively applying combined arms in and across all domains. It provides a flexible means to present multiple

---

[85] Brown, *A Radar History of World War II: Technical and Military Imperatives*, 258.

[86] Alfred Price, *The History of US Electronic Warfare, Volume I "The Years of Innovation-Beginnings to 1946"* (Westford, MA: The Association of Old Crows, 1984), 47-49.

[87] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 426.

[88] US Department of Defense, *Joint Operational Access Concept (JOAC) Version 1.0*, Foreword.

> dilemmas to an enemy by converging capabilities form multiple domains to create windows of advantage, enabling friendly forces to seize, retain, and exploit the initiative to defeat enemies and achieve campaign objectives.[89]

EW made significant contributions and cross domain effects throughout the Guadalcanal campaign. Four events provide examples of EW providing time and space for US commanders across the domains.

First, the landing of the SCR-270 and SCR-268 allowed the Cactus Air Force adequate time to prepare and launch aircraft in time to prevent destruction on Henderson Airfield. The early warning also provided the space required to achieve necessary altitude to gain the advantage against the Japanese bombers as well as mitigate the technical edge the Japanese fighters had against the US aircraft. The two radar systems gave the ground team the ability to vector the pilots and give adequate direction to target enemy aircraft formations enroute to disrupt naval and ground operations on Guadalcanal.

Second, crypto-analysts were able to intercept Japanese radio traffic and provide time and space across all domains allowing Admiral Halsey the opportunity to gain the advantage. The message decrypted on 8 November revealed Admiral Yamamoto's plan to begin a major operation with on 13 November.[90] This valuable intelligence enabled time and space to plan and prioritize efforts for the defense of Guadalcanal. The information proved invaluable to naval commanders in the naval battle for Guadalcanal 13-15 November which prevented Japanese Naval reinforcement even at high cost to US naval assets.

Third, Rear Admiral Lee effectively used the SG radar on the night of 14 November to gain time and space for himself to achieve tactical results and victory. Additionally, his use of the SG radar and eventual denial of Japanese reinforcement gained time and space for the operational

---

[89] US Army Training and Doctrine Command, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040, Version 1.0," October, 2017, accessed October 19, 2017, https://admin.govexec.com/media/20171003_-_working_draft_-_concept_document_for_multi-domain_battle_1_0.pdf.

[90] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 426.

level commander and the 1st Marine Division on the island. The Japanese elements of the 17th Army were denied resupply creating risk of culmination and inability to mount any effective counteroffensive efforts. Additionally, Admiral Turner was able to get 5,529 American reinforcements to Guadalcanal during that same period without loss of transports.[91]

Finally, EW assisted in cross domain effects by providing time and space on 7 December 1942. The coast watchers provided radio warning of a Japanese naval reinforcement effort by 12 destroyers.[92] This timely report allowed both air and naval interdiction. US pilots attacked the convoy of ships on the evening of 7 December and PT boats were launched to interdict the convoy throughout the night. The PT boats are credited with disrupting the convoy operations and causing the Japanese commander, Captain Sato, to abandon the resupply effort on 8 December. In addition, the Americal Division was able to land and reinforce Guadalcanal that same day without loss of ship or Soldier.[93] The continued cross domain success of the US forces across all four domains, provided Admiral Halsey adequate time and space to seize the initiative at all echelons and forced a decision by Japanese operational and strategic leaders to abandon Guadalcanal as an offensive effort and begin the withdrawal.[94]

The fifth question is what can cyber do to integrate cross domain capabilities to buy time and space for the commander? EW was instrumental in identifying enemy aviation and naval assets. The critical information on Japanese locations received in a timely manner allowed both US aviation and naval assets time to prepare. Additionally, economy of force was achieved by providing a critical reconnaissance capability reducing the requirement for aerial assets to expend limited assets and time to find Japanese locations. The combination of radars and coastal watchers provided adequate early warning allowing for pilot rest and conservation of very limited

---

[91] Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, 490.

[92] Ibid., 520.

[93] Ibid.

[94] Ibid., 534.

fuel supplies, thereby reducing maintenance and loss of aircraft.[95] EW assets enabled US commanders at the strategic and operational levels to control the tempo of both the preparation and execution of combat operations across the sea, air and land domains. The ability to control tempo allowed the commanders to prioritize efforts, preserve combat power, capabilities, and strained logistics. Simultaneously, the Japanese had to remain at the extent of their operational reach increasing risk to the mission. The Japanese were forced by necessity to operate at a greater strain to resources, ships,[96] airframes, sustainment, and manpower.

The sixth question is what are the current enemy cyber capabilities and methods of employment at the operational level? The Japanese did possess and employ EW capabilities during World War II and the Guadalcanal campaign. The Marines discovered two Japanese radar sets on Guadalcanal shortly after the landing on 7 August.[97] Japanese radar development lagged behind the United States significantly and the quality was poor as well.[98] Organizational structure and parochialism between the army and navy limited Japanese radar research and development and strained resources.[99] Subsequently, radar employment and effectiveness were limited and lacked full development until after 1943. The radars found on Guadalcanal were early developed radars and most likely a Tachi-6. The Tachi-6 had a range of 185 miles, but had no capability to determine altitude of aircraft,[100] thereby limiting its usefulness for fighter directional control from

---

[95] Brown, *A Radar History of World War II: Technical and Military Imperatives*, 250.

[96] Koburger, *Pacific Turning Point: The Solomons Campaign, 1942-1943*, 119.

[97] Lundstrom, *The First Team and the Guadalcanal Campaign: Naval Fighter Combat from August to November 1942*, quoted in Louis Brown, *A Radar History of World War II: Technical and Military Imperatives*, 248.

[98] Devereux, *Messenger Gods of Battle: Radio, Radar, Sonar, the Story of Electronics in War*, 219.

[99] Price, *The History of US Electronic Warfare, Volume I "The Years of Innovation-Beginnings to 1946,"* 291.

[100] Ibid., 289-290.

a ground station. The poor radar was compounded by low quality radio systems in Japanese aircraft often unable to receive valuable information from a ground targeting or direction officer.

The Japanese did have cryptology and crypto-analysis programs in World War II. The Japanese priority for decryption focused on Soviet diplomatic traffic over US because the Soviet codes were easier to break.[101] Additionally, the Japanese lacked the analytical ability beyond the diplomatic and did not focus on military traffic or interpreting US intentions.[102] The Japanese Navy was able to successfully use radio direction-finding signal intercept for triangulation of US ship formation locations but were proven complacent with protecting their own radio traffic even though they knew the United States had broken Japanese codes.[103] The challenge and failure for the Japanese was to use information gained as time sensitive intelligence at either the operational or tactical level.

The seventh question is what are the contributions to the Deep Battle concept and reflexive control? Soviet Deep Battle was defined in Chapter VII, Attack of PU-36 (Soviet Field Regulation of 1936).

> An attack requires a combination of the most powerful personnel and resources and the preparation of overwhelming superiority in the direction of the main effort. In joint operations by all branches and services, offensive operations must have the objective of simultaneously overwhelming the entire depth of the enemy defense. This can be accomplished as follows: a) by air attacks against the reserves and the rear areas of the enemy defenses; b) by artillery attacks against the entire depth of the enemy "tactical defense zone"; c) by tank penetration into the depth of the tactical defense zone; d) by infantry penetration, accompanied by escort tanks, into enemy positions; e) by advancing mechanized and cavalry units into far rear areas of the enemy; f) by large-scale use of smoke screens to conceal friendly movements and to confuse the enemy in less important sectors. In this way the enemy is to be tied down, encircled, and destroyed in the entire depth of his position.[104]

---

[101] Williamson Murray and Allan R. Millett, eds. *Military Innovation in the Interwar Period* (Cambridge: Cambridge University Press, 1998), 358.

[102] Ibid., 358.

[103] Ibid.

[104] USSR, Military Affairs, *Provisional Field Regulations for the Red Army, Vremennyy Polevoy Ustav, RKKA 1936 (PU 36)* original in Russian, 1937, 1-261, Foreign Broadcast Information Service, June 12, 1986, 52-53, accessed November 1, 2017, handle.dtic.mil/100.2/ADA361873.

EW assets when used appropriately during the Guadalcanal campaign provided US commanders the ability to conduct deep operations across domains within the constraints of the systems used. Radar capabilities provided warning across the depth and breadth of their range. The SCR-270 and 268 provided electronic depth and penetration out to 130 miles providing clarity on the enemy direction and altitude of Japanese air attacks. The closest Japanese airfield, naval base, and command and control (C2) location was the island of Rabaul, approximately 675 miles to the northwest of Guadalcanal. The coast watchers located on Bougainville (192-273 miles from Rabaul) and New Georgia (436 miles from Rabaul) provided additional depth beyond the range of either the US or Japanese radar systems. Additionally, the Marine seizure of the Japanese radars on Guadalcanal restricted the Japanese depth for radar early warning. The second EW asset for analysis is the crypto-analysis. The ability of the US forces to provide accurate and timely information on Japanese plans and operations provided both strategic and operational depth for planning and execution of operations to protect US reinforcement and deny the Japanese the ability to do the same.

Reflexive control was not achievable with EW assets during the Guadalcanal campaign. Reflexive control is "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[105] Neither radio communications, crypto-analysis, radar nor the "Ultra" efforts had the ability to provide the offensive or manipulative enemy decision shaping intended by reflexive control. However, EW efforts did provide the opportunity to intercept and understand enemy plans and operations creating time and space to shape friendly combat power to be adequately prepared in depth to attack the enemy at the decisive point.

The eighth question is what critical capabilities across all domains are linked to cyber capabilities and critical vulnerabilities? Critical capabilities for both belligerents in the

[105] Thomas, *Kremlin Kontrol: Russia's Political-Military Reality,* 176.

Guadalcanal campaign revolved around sustainment. Reinforcement, resupply operations, and available transports and ships (destroyers) determined the ability of both the Japanese and United States to have adequate combat power available across all domains to seize and secure Guadalcanal and Henderson Airfield. The island was critical to further offensive operations and expansion of operational reach. EW assets indirectly impacted the ability to identify, target, prepare, disrupt, delay, and destroy Japanese naval resupply convoy assets. The subsequent shipping and aviation losses continued to mount for the Japanese and they were no longer capable at the strategic and operational levels to restore the ability to project combat power or replace the losses.[106]

Russia in Ukraine 2013-2016

The second case study for analysis is the Russian operations in the Ukraine from 2013-2017. Throughout the remainder of this case study Russia will be assessed as the primary belligerent and the Ukraine will be referred to as the enemy belligerent. Russian decision-making in the Ukraine has demonstrated the ability to use cyber and information warfare to influence operations to support military and political objectives, and continued preparation of the cyber environment to create a range of options for future action.[107] The Russians were able to use the Ukraine operations as a test for New Generation Warfare (NGW) to enhance the deep battle concept. Russia has adeptly executed deep battle, creating time and space to effectively employ limited ground forces and special operations to achieve desired effects. The employment of the cyber domain created windows of opportunity for success and simultaneous execution of offensive and defensive tasks across the strategic and operational levels and other domains.

---

[106] Abdul Karim Baram, *Technology in Warfare: The Electronic Dimension* (Abu Dhabi, United Arab Emirates: Emirates Center for Strategic Studies and Research, 2008), 129.

[107] James R. Clapper, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, February 9, 2016, accessed November 13, 2017, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

Additionally, the cyber capabilities employed have allowed the Russians to achieve three critical strategic effects; 1) troop levels were minimized through integrated cyber operations and operational advantage gained; 2) Russian leadership maintained plausible deniability through effective cyber and information operations delaying international intervention; 3) cyber operations achieved desired effects and kept the threshold for violence below an international outcry for intervention or interference allowing the Russians to achieve the strategic objective to control key terrain in the Ukraine.[108]

Russia has used several techniques to enhance its advantage and gain opportunities to exercise reflexive control and achieve cross-domain synergy and advantage. Russian cyber activities have targeted Ukrainian government, law enforcement, and military officials through cyber espionage,[109] passive intel collection, Distributed Denial of Service (DDoS) attack, integrated local and international information campaigns (using social media, mass media, and internet 'trolls' capacity), undermining of belligerent government and security apparatus institutions, credibility, and effectiveness, and finally has demonstrated the ability to create temporary and permanent effects on the Ukrainian national power grid.[110] Russia's strategy has been to use the information gained from its computer network exploitation campaigns to influence the decision making process and actions, intentionally shape public opinion, distort

[108] Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* June 20, 2017, accessed October 30, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[109] Looking Glass, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare* (Lookingglass Cyber Threat Intelligence Group, CTIG-20150428-01, April 28, 2015), 3, accessed October 30, 2017, https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf.

[110] Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: March, 2016), 1-3, accessed October 29, 2017, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

international perceptions and understanding of the situation to limit timely actions, and maintain its dominant position in Ukraine without international interference.[111]

The first research question is what are cyber capabilities in the defense? Russian cyber capabilities in the defense in the Ukraine are rarely discussed in open source information. Unfortunately, to date, little has been reported about failed cyber-attacks by either side, so it is difficult to identify instances in which defensive cyber countermeasures were successful. Strategically, both Russia and the Ukraine have taken measures to increase the defense of their respective networks.

The Russian response to the potential for cyber retaliation or counterattack has been primarily strategic level actions to limit access to the Russian internet and information apparatus. Russia has invested heavily in cyber capabilities development to break the reliance on foreign company technology. It has made efforts to harden its cyber terrain and passed numerous laws that limit diffusion of cyber access to Russian non-state actors over whom the state may not exercise sufficient control. Finally, Russia has created domestic laws to deny anonymity and ensured all information contained on the Russian internet is physically stored and registered to users.[112]

In addition to strategic level investment in cyber infrastructure and controls on access, cyber has been used as a major focus for a defensive posture in the information war. Russia has used global and regional access through the cyber domain to shape the narrative and political environment. Russia has, "1) developed internally and externally focused media with a significant

---

[111] Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine,* ed. Kenneth Geers (Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015), 67-77, accessed November 9, 2017, https://ccdcoe.org/sites/default/files/multimedia/pdf/cyber warinperspective_full_book.pdf.

[112] Sergei A. Medvedev, "Offense-defense theory analysis of Russian cyber capability" (monograph, Naval Postgraduate School, 2015), 37-40, accessed November 16, 2017, https://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf;sequence=3.

online presence; 2) used social media to guarantee that Russian narratives reach the broadest possible audience; and 3) polished their content in terms of language and presentation so that it rings true in various cultural settings." [113] The Russian ability to capitalize on traditional media, the internet, and social media has allowed them to shape the narrative domestically, regionally, and globally. The broad effort and capabilities allow Russia to control strategic and operational tempo through narrative, confusing the clarity of perceptions and situational understanding for other concerned international actors. The deliberate confusion and counter-narrative undermines the Ukraine Government's credibility while disrupting its ability to communicate with domestic supporters and the global community. Russian actions thus far are in keeping with the NGW and Deep Battle concepts facilitating effective informational environment defense and shaping for offensive operations and reflexive control.

The second question is what is the current US operational approach to the implementation of cyber capabilities at the operational level? Currently the focus of US application of cyber capabilities at the operational level focuses at the linkage among the national cyber strategy in *The DoD Cyber Strategy,* joint documents from JP 3-12 (R) *Cyberspace Operations,* and the recently released US Army tactical doctrine on the application of cyber and electromagnetic capabilities found in FM 3-12 *Cyberspace and Electronic Warfare Operations*. The current failing however, is the lack of operational level documents to link the tactical to the strategic. The particular power of this second case study allows US operational planners to understand a current threat's application of cyber across all three echelons to inform requirements for US cyber operations and lessons learned specifically from the Russian challenges with cyber

[113] Keir Giles, "Working Paper: Russia's Hybrid Warfare: a Success in Propaganda," European Security and Defence College, 18 February 2015, quoted in James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015), 36, accessed November 9, 2017, https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

at the operational level. These will be discussed more in depth throughout the remainder of this case study as well as in the analysis and findings section. Cyber capabilities offer significant opportunities to the force that can integrate effectively across all domains to gain temporary windows of advantage, improve operational reach, control tempo at echelon, and link tactical actions in time and space during a campaign to achieve strategic effects efficiently.

The third research question is what are the cyber capabilities in the offense? Russia has effectively implemented cyber capabilities within the deep operations concept and its modern evolution of NGW. Russian operations in the Ukraine have provided a valuable practical exercise in cyber use within a limited conflict to achieve tactical, operational, and strategic objectives. During the outset of Russian operations in the Ukraine in 2014, security experts accurately predicted the Russian cyber strategy will be a higher evolution in sophistication than the previous Russian attacks against Estonia in 2007 and Georgia in 2008, and that "Moscow is more likely to use narrowly focused, limited operations in support of strategic state objectives."[114] Russia has used a myriad of methods and has achieved mixed results with a decentralized application of proxy cyberwarfare, use of malware, advanced persistent threats (APTs), and DDoS.

The most notable proxy hacker incident occurred during the Ukrainian Presidential election in May of 2014. CyberBerkut, a pro-Russian hacktivist group, launched a cyberattack against the Ukraine's Central Election Commission computers and posted false election results with a synchronized effort from Russian TV Channel One corroborating the false reports.[115] The attacks undermined the credibility of the Ukrainian government domestically, regionally, and internationally. Additionally, the results also provided fuel to support the Russian narrative that

---

[114] Jen Weedon and Laura Galante, "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast," FireEye Executive Perspectives, March 12, 2014, accessed November 13, 2017, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russiahackers-cyberwar-not-so-fast.html.

[115] Nolan Peterson, "How Russia's Cyberattacks Have Affected Ukraine," December 16, 2016, accessed October 30, 2017, http://dailysignal.com/2016/12/16/how-russias-cyberattacks-have-affected-ukraine/.

the ethnic Russian separatists were fighting corruption and needed help from Russia to achieve independence and protect their rights. The hackers displayed unique sophistication, conducting in-depth system reconnaissance two months prior, gaining administrator-level access to the election commission network, and employing advanced cyber espionage malware (Sofacy/APT28/Sednit).[116]

In addition to interfering with the Ukrainian 2014 election, Pro-Russian hacker groups have claimed responsibility for additional cyber events: the disruption of German government websites, intercept of US and Ukrainian military cooperation documents, DDoS attacks against NATO websites, blocking of Ukrainian government and media websites, and various negative messaging campaigns slandering pro-Ukrainian supporters.[117] CyberBerkut is also actively undermining Ukrainian legitimacy and credibility for governance by attacking ineffective infrastructure management and the threat of nuclear power reactor failure. Additionally, they are publishing stories to discredit US credibility through ties of the Clinton Foundation to Ukrainian misuse of International Monetary Fund (IMF) funds.[118]

The Russians launched sophisticated malware attacks against Ukrainian targets, such as a Snake/Uroboros malware exploitation of government computers, disrupted telecommunications infrastructure, and jamming of Ukrainian parliamentarians' cell phones.[119] A deliberate cyber-espionage campaign known as 'Operation Armageddon,' has been active since mid-2013

---

[116] Nikolay Koval, "Revolution Hacking," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015), 36, accessed November 9, 2017, https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

[117] Sergei A. Medvedev, "Offense-defense theory analysis of Russian cyber capability," 26.

[118] CyberBerkut, accessed November 16, 2017, https://cyber-berkut.org/en/.

[119] Sergei A. Medvedev, "Offense-defense theory analysis of Russian cyber capability," 28. See also Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015), 73, accessed November 9, 2017, https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

targeting Ukrainian military, government, and law enforcement officials to gain intelligence concerning Ukrainian strategic, operational, and tactical plans.[120] A recent study identified two major classifications of target groups for the Russian attacks. Prior to the conflict, during shaping operations, the targets were the Ukrainian government officials, members of the opposition, and pro-opposition journalists. Once ground operations began the second target group included Ukrainian government and law enforcement focusing on those involved or located near Russian rebel operations.[121]

The fourth question is what are examples of cross domain effects providing time, space and operational advantage? There are four primary examples from the Russian operations in the Ukraine: 1) phase zero information shaping operations, 2) cyber operations to disrupt and deny Ukrainian command and control; 3) SOF operations integrated with cyber to seize key physical and cyber terrain, and 4) cyber-espionage operations to gain operational and tactical advantage. First, the cyber/information warfare prior to the beginning of ground combat operations created strategic paralysis of international actors and the Ukraine to create time and space for the Russian operational and tactical level commanders to seize key terrain, install rebel leadership, and create and promulgate a viable information campaign to support operations. Second, at the outset of the ground combat operations critical communication infrastructure was attacked with cyber capabilities to deny Ukrainian government agency communication and military command and control.[122] The cyber and information operations set the conditions for the third application. As the invasion progressed, Russian intelligence and special operations forces created cross domain effects through a raid on critical Ukrainian internet infrastructure. The ground forces installed

---

[120] Looking Glass, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare,* 3.

[121] Ibid., 8.

[122] The Institute for National Security Studies (INSS), "The Ukrainian crisis- a cyber warfare battlefield," *Defense Update*, April 5, 2014, accessed November 16, 2017, http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html.

data intercept devices and physically isolated Ukrainian internet and telecommunications infrastructure.[123] Finally, cyber-espionage has gained valuable intelligence through cyber reconnaissance to provide information on Ukrainian government, military and law enforcement planning and operations.[124] This actionable intelligence was used to create time and space, as well as maneuver and fires advantage to the Russian-backed rebels.

The fifth question is what can cyber do to integrate cross domain capabilities to buy time and space for the commander? Cyber capabilities are an effective tool at the operational level to create paralysis in the command and control architecture of an opponent. In addition, strategically it can provide temporary windows of advantage through a strategic narrative and coordinated information operations to prevent the international community from understanding the operational environment, thereby creating strategic paralysis and either a delayed or complete lack of response from potential alliance partners. Next, cyber operations can create time and space at the operational and tactical level through reconnaissance. The intelligence collection provides a detailed understanding of an opponent's plan allowing commanders to shape operations with fires and maneuver to destroy an unsuspecting enemy.

The sixth question is what are the current enemy cyber capabilities and methods of employment at the operational level? Ukraine's struggle with effective cyber defense against an able opponent, creates a framework and mirror for the cyber weaknesses of other international actors against a possible Russian cyber-attack. Ukrainian cyber capabilities, although less equipped than Russia's, still include significant assets and highly trained personnel. Ukraine

[123] Sergei A. Medvedev, "Offense-defense theory analysis of Russian cyber capability," 29.

[124] Looking Glass, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare,* 3.

suffers from a lack of a cyber legal framework,[125] a coherent strategy[126] and operational linkage from the tactical application of available cyber assets and capabilities. Until a legal framework can be established within Ukraine and government agencies created, manned and trained effectively the majority of critical national infrastructure will rely on private sector approaches to effectively defend against Russian cyber-attacks.[127] Ukraine relies on reactive defensive capabilities as it hastily builds a structure which can provide a proactive approach and response.

The evolution of Russian capabilities between the two power grid attacks in December of 2015 and 2016 provide poignant lessons in cyber defense.[128] The advanced malware, extensive cyber-espionage and lengthy reconnaissance, and specifically the ability to highjack multiple power stations Supervisory Control and Data Acquisition (SCADA) systems demonstrate significant capabilities. The attack required a manual override of the system by Ukraine to bring the power grids back online.[129] Russian hackers were able to use the supervisory role and remote through the system to gain access and control multiple switches and bypass Ukrainian cyber monitors and defense capabilities. The attacks demonstrate Russian ability to potentially permanently disrupt power to 100,000 users. Within the Ukraine, a power outage during the winter would create permanent infrastructure damage and loss of life. The demonstration provides an additional punitive coercive capability to force compliance and potential

---

[125] Jan Stinissen, "A Legal Framework for Cyber Operations in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015), 123-134, accessed November 9, 2017, https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

[126] Nadiya Kostyuk, "Ukraine: A Cyber Safe Haven?," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015), 122, accessed November 9, 2017, https://ccdcoe.org/sites/default /files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

[127] Ibid, 117.

[128] Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* June 20, 2017.

[129] Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 24.

weaponization with catastrophic effects from cyber to physical domains and on a civilian population. Ukraine has made efforts to work with outside agencies to assist in identifying weaknesses within their systems, but is still struggling to develop solutions.

The seventh question is what are the contributions to the Deep Battle concept and reflexive control? Russian attacks in the Ukraine have provided recent examples of the evolution of Russian Operational Art and testing of the modern, hybrid or new generation warfare.[130] The effective employment of cyber capabilities has proven to create time and space across all three echelons of war. *Udar* or operational shock was achieved across every level within the enemy system (Ukraine) for decision making and C2. Additionally, cyber capabilities integrated with the Russian strategic information campaign achieved unprecedented strategic level shock limiting the international community's understanding of the situation and greatly limiting the response. The shock achieved set the conditions for operational and tactical maneuver enabling the Russians to quickly seize key terrain within the Ukraine through rebels with minimal Russian footprint of unmarked and unclaimed special operations forces.

Reflexive control has accomplished significant strategic and operational integration to achieve the desired Russian end state in the Ukraine to control key terrain and gain access while limiting international interference. Maria Snegovaya, a leading expert on Russia and the Ukraine, identified the following five key elements of Russia's reflexive control techniques used in the Ukraine:

> • Denial and deception operations to conceal or obfuscate the presence of Russian forces in Ukraine, including sending in "little green men" in uniforms without insignia;
> • Concealing Moscow's goals and objectives in the conflict, which sows fear in some and allows others to persuade themselves that the Kremlin's aims are limited and ultimately acceptable;
> • Retaining superficially plausible legality for Russia's actions by denying Moscow's involvement in the conflict, requiring the international community to

[130] Andrew Monaghan, "Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare,' *Parameters* 45, no. 4 (Winter 2015-16): 65-74, accessed October 30, 2017, http://ssi.armywarcollege.edu /pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf.

> recognize Russia as an interested power rather than a party to the conflict, and pointing to supposedly-equivalent Western actions such as the unilateral declaration of independence by Kosovo in the 1990s and the invasion of Iraq in 2003;
> • Simultaneously threatening the West with military power in the form of overflights of NATO and non-NATO countries' airspace, threats of using Russia's nuclear weapons, and exaggerated claims of Russia's military prowess and success;
> • The deployment of a vast and complex global effort to shape the narrative about the Ukraine conflict through formal and social media.[131]

A significant emerging aspect is Russia's effective use of cyber-espionage. An emerging aspect of reflexive control is the effective use of cyber reconnaissance to gain intelligence and understanding of the enemy's plans in detail. Rather than controlling the enemy's response, the Russians have been able to understand Ukrainian plans and shape their fires and maneuver to destroy Ukrainian forces and support Russian backed rebels to achieve their objectives.

The eighth question is what critical capabilities across all domains are linked to cyber capabilities and critical vulnerabilities? JP 5-0 defines critical capabilities as the "primary abilities essential to the accomplishment of the objective." Critical requirements are "essential conditions, resources, and means the COG requires to perform the critical capability." Critical vulnerabilities are "those aspects or components of critical requirements that are deficient or vulnerable to direct or indirect attack in a manner achieving decisive or significant results."[132] The most critical capability to date has been the Russian information warfare apparatus and integrated NGW concept and execution. Russia's critical requirements have been its myriad of cyber capabilities. Specific Russian capabilities include: proxy hackers, cyber espionage capabilities within the Russia and Ukraine, social media internet 'trolls,' and an effective operational level approach to the integration of cyber capabilities to synchronize and link tactical actions in time and space to

---

[131] Maria Snegovaya, "Russia Report I: Putin's Information Warfare in Ukraine," Institute for the Study of Warfare: September 2015, 7, accessed October 30, 2017 http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

[132] US Joint Staff, JP 5-0, (2017), IV-25.

the strategic aims. Russia's critical vulnerability is the integrity, legitimacy, and credibility of the information campaign and a counter narrative from the Ukraine.

This case study has highlighted the Russian operational approach to date and the evolution of the Russian operational art and concepts of deep battle and reflexive control. The next section, findings and analysis, will provide insight into an operational approach and framework to counter the Russian strategy and operational approach with respect to cyber domain capabilities applied within Russian New Generation Warfare.

Findings and Analysis

This section includes a structured focus comparison of the US Guadalcanal campaign in May 1942-February 1943 and the Russian campaign in the Ukraine from 2013-2017 using empirical data assembled from the case studies. The comparison will be covered in two separate sub-sections. The findings portion will compare the data gathered in response to the study's eight research questions. The analysis portion will use the results of the findings to test the study's three hypotheses. This section will demonstrate trends in how military forces employ domain capabilities to gain cross domain advantage and create cross domain synergy and temporary windows of advantage exercising operational art to link tactical operations to strategic goals.

Findings

The study's first question is: what are cyber capabilities in the defense? Throughout the campaign for Guadalcanal, five major EW/intel capabilities assisted in gaining cross-domain advantage in the defense. The various radars provided early warning of enemy air and naval assets maneuvering to attack Guadalcanal. The radars allowed US operational leaders to preserve combat power, control operational tempo, and maximize capabilities at decisive points against the Japanese center of gravity. Radio cryptology provided valuable intelligence, similar to cyber-espionage used by the Russians, to determine enemy courses of action, locations of leadership, and critical assets to focus operational assets to achieve maximum effects. The Russian use of

cyber in the defense has focused on limiting access to the Russian internet and information apparatus and using the cyber domain to shape the narrative and political environment, domestically, regionally, and internationally. The broad effort and capabilities allow Russia to control strategic and operational tempo through narrative confusing the clarity of perceptions and situational understanding for other concerned international actors.

The second question is: what is the current US operational approach to the implementation of cyber capabilities at the operational level? The goal of the application of cyber capabilities in the joint targeting process is to synchronize simultaneous and complementary effects across domains to gain a position of advantage and cross domain synergy. During Guadalcanal, EW assets effectively assisted air, land, and sea domains with directional finding capabilities, early warning, and espionage. Similarly, Russians have used cyber capabilities at the operational level to minimize footprint; control physical, cyber, and human terrain; and shape the information environment by controlling tempo, shaping enemy action, and focusing lethality and combat at the decisive point to attack the enemy COG.

The third question is: what are the cyber capabilities in the offense? During Guadalcanal the 40-45 minutes warning provided by radars gave adequate time for the pilots to get their aircraft to the required altitude to contest the bombers and the zeros. Second, the ELINT effort would become a shaping operation for future island hopping to establish the conditions for amphibious landings as the Japanese radars became a target for identification of Japanese defenses. Finally, communications intelligence (COMINT) provided early warning of the major Japanese operations. Russia has effectively implemented cyber capabilities within the deep operations concept and its modern evolution of New Generation Warfare. Russia has used a myriad of methods and has achieved results with application of proxy cyberwarfare, use of malware, advanced persistent threats (APTs), and DDoS. The attacks undermined the credibility of the Ukrainian government domestically, regionally, and internationally. Sophisticated malware attacks were also launched against Ukrainian targets, such as a Snake/Uroboros malware

exploitation of government computers, disrupted telecommunications infrastructure, and jamming of Ukrainian parliamentarians' cell phones impacting the tempo of Ukrainian operations and ability to make decisions and conduct command and control activities.[133] The Russian cyber-espionage campaign known as 'Operation Armageddon,' has allowed them to shape the operational environment by disrupting Ukrainian leadership ability to command and control, determining Ukrainian tactical and operational level plans, disrupting Ukrainian operations, and focusing combat power to destroy Ukrainian forces based on cyber intercepts of Ukrainian force and leader locations.

The fourth question is: what are examples of cross domain effects providing time, space and operational advantage? At Guadalcanal the joint force routinely used a combination of capabilities within the air, land, sea and EW domains to increase efficiency and effectiveness. Both US and Japanese forces were operating at the extent of operational reach and near culmination. The efficiencies gained through EW application assisted in preserving manpower and equipment while simultaneously maximizing combat power at the decisive point against the Japanese COG of sustainment operations. Russia was able to achieve cross domain synergy with multiple aspects. The largest strategic payoff came from minimizing overall footprint and creating international fog and friction impacting strategic decision-making tempo for outside actors. The coordinated information operations through cyber and media created time and space operationally to seize key objectives in the physical terrain with minimal troop levels required. Russian cyber espionage forced Ukrainian culmination through gaining intelligence to strike Ukrainian command and control, tactical units, and decision-making processes. Russian exploitation of temporary windows of advantage within the digital domain created opportunities to control and exploit tempo at all echelons.

---

[133] Sergei A. Medvedev, "Offense-defense theory analysis of Russian cyber capability," 28. See also Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," 73.

The fifth question is: what can cyber do to integrate cross domain capabilities to buy time and space for the commander? EW assets enabled the US commanders during the fight for Guadalcanal to control the tempo of both the preparation and execution of combat operations across the sea, air and land domains. The ability to control tempo allowed the commanders to prioritize efforts and preserve combat power, capabilities, and strained logistics. Simultaneously, the Japanese had to remain at the limit of their operational reach increasing risk to the mission. The Japanese were forced by necessity to operate at a greater strain to resources. Operations in the Ukraine offer additional lessons on application of cyber capabilities as an effective tool to create paralysis within the enemy's command and control architecture. Additionally, cyber capabilities can provide temporary windows of advantage through coordinated information operations to prevent the international community from understanding the operational environment, thereby creating strategic paralysis and either a delayed or a complete lack of response from potential adversary partners. Through cyber reconnaissance, intelligence collection provides a detailed understanding of an opponent's plan allowing commanders to shape operations with fires and maneuver to destroy an unsuspecting enemy.

The sixth question is: what are the current enemy cyber capabilities and methods of employment at the operational level? The Japanese did possess and employ EW capabilities during the Guadalcanal campaign. The Japanese lacked an integrated national research, development and procurement program. Organizational structure and parochialism between the army and navy limited Japanese radar research and development and strained resources.[134] The Japanese military culture also lacked a focus for the use of crypto-intelligence and building a force structure to facilitate collection and exploitation. The challenge and failure for the Japanese was to use information gained as time sensitive intelligence at either the operational or tactical

[134] Price, *The History of US Electronic Warfare, Volume I "The Years of Innovation-Beginnings to 1946,"* 291.

level. Ukraine continues to struggle to establish an effective cyber defense against an able opponent. Ukrainian cyber capabilities, although less equipped than Russia, still include significant assets and highly trained personnel. The Ukraine suffers from a lack of a cyber legal framework,[135] a coherent strategy,[136] and operational linkage from the tactical application of available cyber assets and capabilities. Until a legal framework can be established within Ukraine and government agencies created, manned and trained effectively the majority of critical national infrastructure will rely on private sector approaches to effectively defend against Russian cyber-attacks.[137] Ukraine is reliant on reactive defensive capabilities as it hastily works to build a structure which can provide a proactive approach and response.

The seventh question is: what are the contributions to the Deep Battle concept and reflexive control? Both case studies demonstrated the effective use of cross domain capabilities to gain synergy and synchronize assets within and across multiple domains. The efficiencies gained allowed operational and strategic commanders the opportunity to prioritize assets and minimize force used to maximum affect against the enemy at the critical time and decisive points to attack the enemy's COG. During the campaign for Guadalcanal, EW assets provided US commanders the ability to conduct deep operations across multiple domains within the constraints of the systems used. Radar capabilities, coupled with coast watchers, provided warning across the depth and breadth of their range. Additionally, the Marine seizure of the Japanese radars on Guadalcanal restricted the Japanese depth for radar early warning. The ability of crypto-analysts to provide accurate and timely information on Japanese plans and operations provided both strategic and operational depth for planning and execution of operations to protect US reinforcement and deny the Japanese the ability to do the same. The Russians achieved

---

[135] Stinissen, "A Legal Framework for Cyber Operations in Ukraine," 123-134.

[136] Kostyuk, "Ukraine: A Cyber Safe Haven?," 122.

[137] Ibid., 117.

operational shock across every level within the Ukrainian C2 and decision-making system. The effective employment of cyber capabilities has proven to create time and space across all three echelons of war. Additionally, cyber capabilities integrated with the Russian strategic information campaign achieved unprecedented strategic level shock limiting the international community's understanding of the situation and creating adequate fog and friction to prevent a coherent and timely response. The shock achieved set the conditions for operational and tactical maneuver enabling the Russians to quickly seize key terrain within the Ukraine.

The eighth question is: what critical capabilities across all domains are linked to cyber capabilities and critical vulnerabilities? Critical capabilities for both belligerents in the Guadalcanal campaign revolved around sustainment. Reinforcement, resupply operations, and available transports and ships (destroyers) determined the ability of both the Japanese and United States to have adequate combat power available across all domains to seize and secure Guadalcanal and Henderson Airfield. The island was critical to conduct offensive operations and expand operational reach. EW assets indirectly impacted the ability to identify, target, prepare, disrupt, delay, and destroy Japanese naval resupply convoy assets. In the Ukraine the most critical capability to date has been the Russian information warfare apparatus and integrated NGW concept and execution. The critical requirements for the Russians have been their myriad of cyber capabilities. Russian capabilities include: proxy hackers, cyber espionage capabilities within Russia and Ukraine, social media internet 'trolls,' and an effective operational level approach to the integration of cyber capabilities to synchronize and link tactical actions in time and space to the strategic aims. Russia's critical vulnerabilities are the integrity, legitimacy, and credibility of the information campaign and a counter narrative from the Ukraine.

Analysis

This study relied on three hypotheses. First, when an operational approach arranges cyber capabilities across all domains it will create time and space allowing the operational level

commander to shape the deep fight and control the tempo of joint operations. The evidence suggests this hypothesis is supported. Both the United States at Guadalcanal and Russia in the Ukraine demonstrate the operational commander's use of cyber and EW capabilities to create cross domain advantage and synergy. The efforts created critically needed time to prioritize limited assets, capabilities, and manpower. Operational level leaders were able to mitigate risk and apply combat power at critical decisive points, using an indirect approach to attack the enemy COG. The applied cyber and EW assets prevented US and Russian culmination while operating at the limit of operational reach and consequently forced the opponent to culminate and conduct costly operations beyond his operational reach.

Second, when cyber capabilities are used across all domains they provide the operational commander time and space in the defense to expose and increase enemy vulnerability by forcing the enemy to concentrate forces. The evidence suggests this hypothesis is also supported. Both case studies illuminate critical lessons for operational commanders in the defense. Operational commanders assume the defense to regenerate combat power and build capabilities to regain the offense. At Guadalcanal Halsey was able to gain time and create tactical, operational, and strategic space by defending and contesting critical sea lanes allowing US resupply and reinforcement and denying the same to the Japanese on the island. The Russians effectively used cyber capabilities in a proactive defense through information operations to prevent international interference with operations. The Russians successfully conducted a strategic cyber defense through cyber and information operations while shaping the environment and conducting minimal force offensive operations to seize key terrain during initial ground operations.

Third, when cyber capabilities are employed across all domains the arrangement achieved will allow operational commanders the time, space and ability to seize, retain, and exploit the initiative, gaining the advantage against the threat. The evidence suggests this hypothesis is supported as well. Both Guadalcanal and the Ukraine demonstrate the use of cyber and EW capabilities to set the conditions to seize the initiative. Cyber and EW allow simultaneity and

depth when used across the other four domains that cannot be achieved without them. The cross-domain synergy achieved in both case studies provided multiple options for the operational commander, created shock and delay in the enemy decision-making cycle, and allowed the Russians and Americans to gain and maintain the initiative forcing operational level culmination of the opponent.

In summation, the evidence from the case studies suggests that all three hypotheses are supported and that the United States during the campaign for Guadalcanal and Russia in the Ukraine have applied operational art to link tactical action to the desired strategic end state. Cyber and EW capabilities are critical in warfare and allow operational level commanders the opportunity to shape the deep fight and control the tempo of multi-domain, joint operations. An effective operational approach will provide the operational commander the opportunity to create temporary windows of advantage by leveraging the cyber and EW domain across other domains.

Conclusion

This research sought to determine how cyberwarfare applied through the lens of operational art contributes to cross domain synergy within the context of multi-domain battle. Cyber and EW capabilities are critical to enable operational commanders the opportunity to create temporary windows of advantage, shape the deep fight, control tempo of multi-domain operations, and arrange cyber effects in time and space to achieve strategic objectives. The three hypotheses this study evaluated support this thesis. First, when an operational approach arranges cyber capabilities across all domains it will create time and space allowing the operational level commander to shape the deep fight and control the tempo of joint operations. Second, when cyber capabilities are used across all domains they provide the operational commander time and space in the defense to expose and increase enemy vulnerability by forcing the enemy to concentrate forces. Third, when cyber capabilities are employed across all domains the arrangement achieved

will allow operational commanders the time, space and ability to seize, retain, and exploit the initiative, gaining the advantage against the threat.

This research used a structured focused approach to evaluate the application of CEMA capabilities within the context of multi-domain battle. The two case studies, the Guadalcanal Campaign 1942-1943 and Russia in the Ukraine 2013-2016, were developed and analyzed with a structured focus comparison of the established eight research questions. Both case studies demonstrate cross domain synergy achieved with successful application of CEMA to provide opportunities and create temporary windows of advantage during multi-domain operations.

The analysis of the three hypotheses provided critical lessons for operational level commanders and planners to maximize the effects of cyber and electromagnetic capabilities to mitigate risks and create opportunities to apply combat power against the enemy's COGs across multiple domains. The achieved additive effects of cross domain synergy are larger than the total sum of the individual parts. Both case studies demonstrate that the multi-domain efforts created critically needed time to prioritize limited assets, capabilities, and manpower. Leaders were able to mitigate risk and apply combat power at critical decisive points, using an indirect approach to attack enemy COGs while preventing their culmination while operating at the limit of operational reach and consequently forced the opponent to culminate and conduct costly operations beyond his operational reach.

Next, when cyber capabilities are used across all domains they provide the operational commander time and space in the defense to expose and increase enemy vulnerability by forcing the enemy to concentrate forces. Operational commanders can gain time and create tactical, operational, and strategic space by defending and contesting critical lines of communication in order to allow US resupply and reinforcement in the rear and close fight and denying the same to the enemy in the deep fight. Additionally, cyber capabilities can be employed in a proactive defense through information operations to prevent international interference with operations. A strategic cyber defense using cyber and information operations will assist in shaping the

environment and reduce force requirements for offensive operations to seize key terrain during initial ground operations.

Finally, when cyber capabilities are employed across all domains the arrangement achieved allows commanders the time, space and ability to seize, retain, and exploit the initiative, gaining the advantage against the threat. Cyber and EW capabilities allow simultaneity and depth when used across the other four domains that cannot be achieved without them. The cross-domain synergy achieved in both case studies provided multiple options for the operational commander, created shock and delay in the enemy decision-making cycle, and allowed the Russians and Americans to gain and maintain the initiative forcing operational level culmination of the opponent.

Future studies should evaluate cross domain synergy and the ability to achieve simultaneous effects through the integration of all domains with the inclusion of MISO as a major component. An investigation of the application of the Russian New-Type of War with the All-Inclusive Command and Control of Combat Operations will allow strategic and operational level leaders to develop wargames against a near peer threat and specifically the Russian model for wargames and planning exercises. Additionally, classified research will provide a more robust study and in-depth analysis supported by cyber experts to provide technical requirements to appropriately combat Russian cyber threats. Finally, a combatant command, in partnership with US Cyber Command, should undertake a planning effort and command post exercises to test capabilities and potential operational approaches to combat cyber threats during combat operations. These future studies will assist and inform in the cyber capabilities and future requirements across doctrine, organization, training, materiel, leadership and education, personnel, facilities (DOTMLPF) required to enable the joint force to fight and win our nation's wars.

Appendix 1: Figures

Figure 1. Methods and Ways of Conducting a New-Type of War, *Military Review* (July-August 2017): 40.

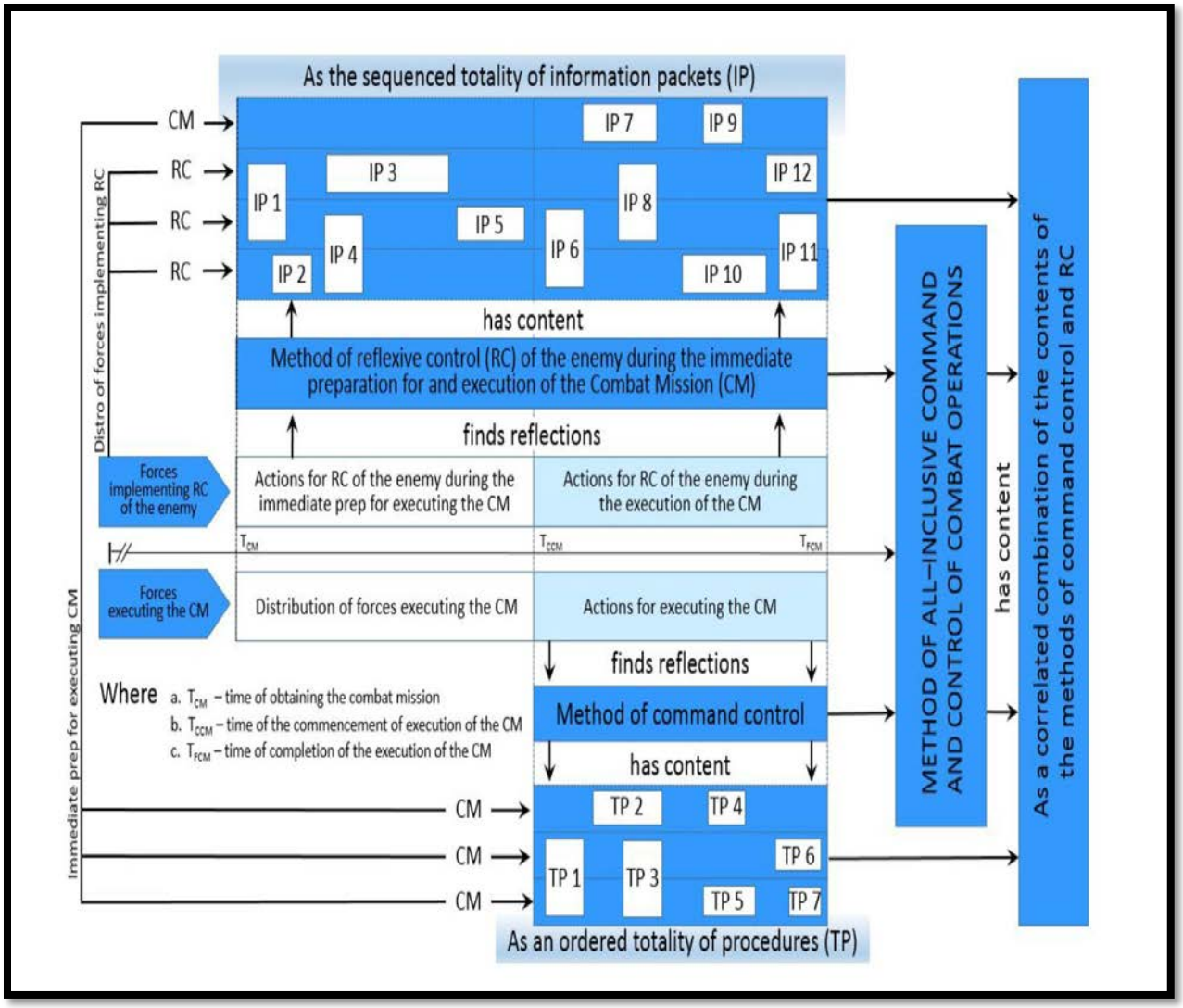

Figure 2. Russian Concept of All-Inclusive Command and Control of Combat Operations, *Kremlin Kontrol: Russia's Political-Military Reality*, 195.

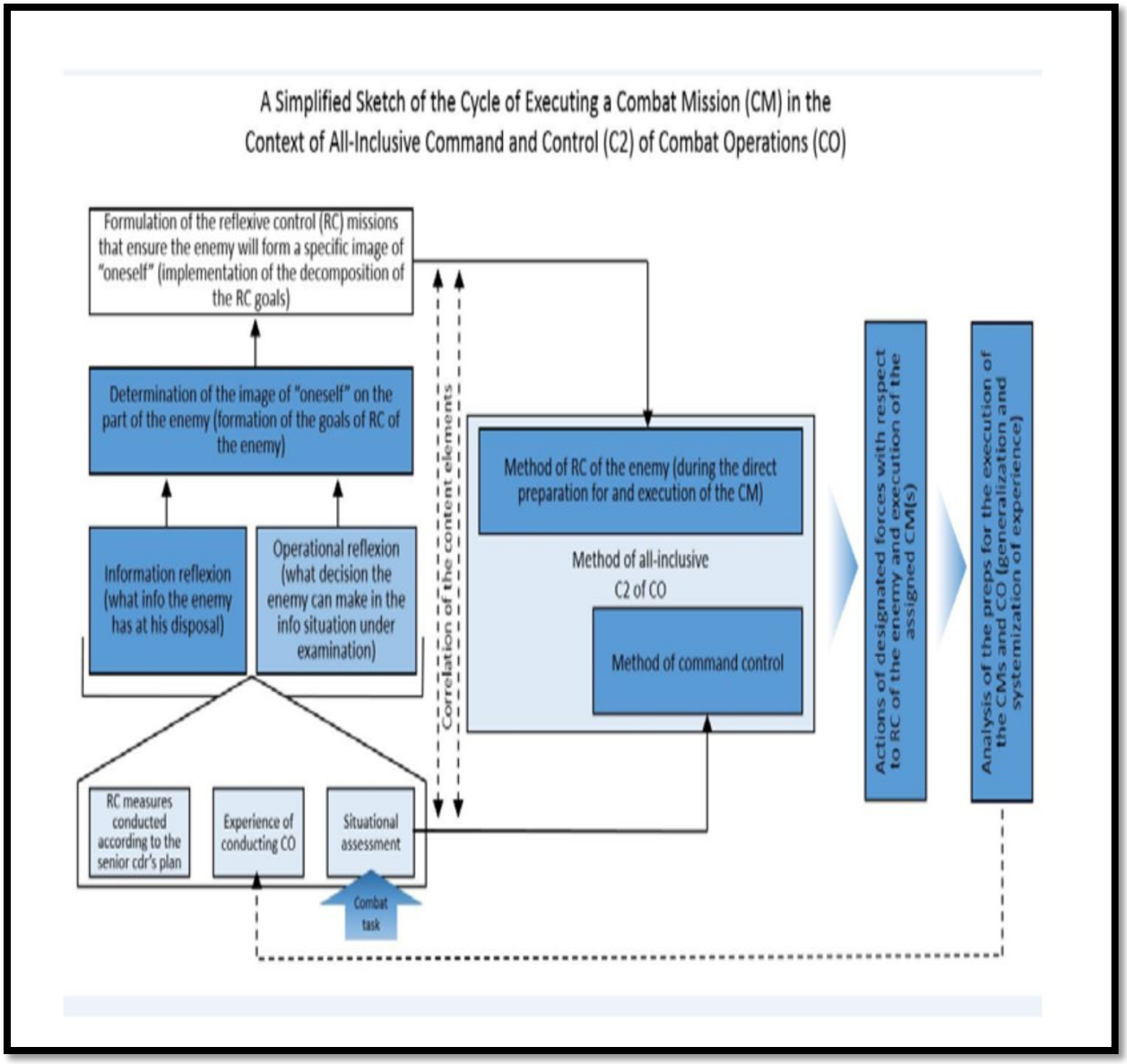

Figure 3. Russian Concept of All-Inclusive Command and Control of Combat Operations, *Kremlin Kontrol: Russia's Political-Military Reality*, 196.

Bibliography

Baram, Abdul Karim. *Technology in Warfare: The Electronic Dimension*. Abu Dhabi, United Arab Emirates: Emirates Center for Strategic Studies and Research, 2008.

Bartsch, William H. *Williams-Ford Texas A&M University Military History Series*. Vol. 147, *Victory Fever On Guadalcanal: Japan's First Land Defeat of World War II*. College Station: Texas A&M University Press, 2014.

Beasley, W. G. *Japanese Imperialism, 1894-1945*. Oxford, Oxfordshire: Clarendon Press, 1987.

Bott, Jonathan. "Outlining the Multi-Domain Battle Concept." June 8, 2017. Accessed August 19, 2017. https://overthehorizonmdos.com/2017/06/08/outlining-the-multi-domain-operating-concept/.

Brown, Louis. *A Radar History of World War II: Technical and Military Imperatives*. Bristol: Institute of Physics Pub., 1999.

Carlisle, Rodney. *Encyclopedia of Intelligence and Counterintelligence*. London, England: Routledge, 2015. Accessed October 31, 2017. http://ebookcentral.proquest.com/lib/columbia/detail.action?docid=2005326.

Clausewitz, Carl von. *On War*. Translated and edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Clapper, James R. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee, February 9, 2016. Accessed November 13, 2017. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

Chapple, Mike and David Seidl. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones and Bartlett Learning, 2015. Accessed August 19, 2017. https://books.google.com/books?id=EVwtBAAAQBAJ&printsec=frontcover&dq=cyber warfare&hl=en&sa=X&ved=0ahUKEwi2-u695uTVAhUp74MKHXYTDU0Q6AEITzAG#v=onepage&q=cyberwarfare%20defined&f=false.

Collier, David. "Comparative Historical Analysis: Where Do We Stand?" *American Political Science Association: Comparative Politics Newsletter*, 10 (Winter 1999): 1-5.

Corera, Gordon. *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage*. New York: Pegasus Books, 2016.

CyberBerkut. Last modified November 16, 2017. Accessed November 16, 2017. https://cyber-berkut.org/en/.

DeBlanc, Jefferson J. *The Guadalcanal Air War: Col. Jefferson Deblanc's Story*. Gretna, LA: Pelican Pub., 2008.

Devereux, Tony. *Messenger Gods of Battle: Radio, Radar, Sonar, the Story of Electronics in War*. London: Brassey, 1991.

Echevarria, Antulio J. "American Operational Art, 1917-2008." In *The Evolution of Operational Art: From Napoleon to the Present*, edited by John Andreas Olsen and Martin van Creveld, 137-165. New York: Oxford University Press, 2011.

Epstein, Robert M. *Napoleon's Last Victory and the Emergence of Modern War*. Modern War Studies. Lawrence: University Press of Kansas, 1994.

Electricity Information Sharing and Analysis Center. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Last modified March, 2016. Accessed October 29, 2017 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Frank, Richard B. *Guadalcanal: The Definitive Account of the Landmark Battle.* New York: Random House, 1990.

Foxall, Andrew. *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*. Russia Studies Centre Policy Paper No. 9, London, Henry Jackson Society, 2016. Accessed November 16, 2017. https://www.stratcomcoe.org/download/file/fid/5212.

Gat, Azar. *A History of Military Thought*. New York: Oxford University Press, 2001.

George, Alexander L. *Case Studies and Theory Development in the Social Sciences*. Besia Studies in International Security. Cambridge, MA: MIT, Press, 2005.

Giles, Keir. "Working Paper: Russia's Hybrid Warfare: a Success in Propaganda," European Security and Defence College, 18 February 2015. Quoted by James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers, 19-28. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015. Accessed November 9, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

Goldstein, Avery. *Rising to the Challenge: China's Grand Strategy and International Security*. Studies in Asian Security. Stanford, CA: Stanford University Press, 2005.

Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar." *Wired*, June 20, 2017. Accessed October 30, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

Hixon, Carl K. *Guadalcanal: An American Story*. Annapolis, MD: Naval Institute Press, 1999.

Isserson, G. S. *The Evolution of Operational Art*. 2nd ed. Translated by Bruce Menning. Fort Leavenworth, KS: Combat Studies Institute Press, US Army Combined Arms Center, 2013.

Jersey, Stanley Coleman. *Texas A&M University Military History Series*. Vol. 111, *Hell's Islands: The Untold Story of Guadalcanal*. College Station: Texas A&M University Press, 2008.

Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Kartapolov, Andrey V. "Lessons of Military Conflicts and Prospects for the Development of Resources and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts." *Vestnik Akademii Voennykh Nauk 2* (*Journal of the Academy of Military Science)* 2 (2015): 35. In Timothy Thomas, "The Evolving Nature of Russia's Way of War." *Military Review* (July-August 2017): 34-42.

Kelly, Justin, and Mike Brennan. “The Leavenworth Heresy and the Perversion of Operational Art.” *Joint Force Quarterly* 56 (January 2010): 109-116. Accessed August 12, 2017. https://cgsc.blackboard.com/webapps/blackboard/execute/content/file?cmd=view&content_id=_540320_1&course_id=_7174_1.

Kipp, Jacob W. “The Tsarist and Soviet Operational Art, 1853-1991.” In *The Evolution of Operational Art: From Napoleon to the Present*, edited by John Andreas Olsen and Martin van Creveld, 64-95. New York: Oxford University Press, 2011.

Koburger, Charles W. *Pacific Turning Point: The Solomons Campaign, 1942-1943*. Westport, CT: Praeger, 1995.

Kostyuk, Nadiya. “Ukraine: A Cyber Safe Haven?” In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 113-122. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015. Accessed November 9, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full _book.pdf.

Koval, Nikolay. “Revolution Hacking.” In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 55-58. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015. Accessed November 9, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full _book.pdf.

Lee, Robert Edward. *Victory at Guadalcanal*. Novato, CA: Presidio Press, 1981.

Leonhard, Robert R. *Fighting by Minutes: Time and the Art of War*. Westport, CT: Praeger, 1994.

Li, Jennifer J., and Lindsay Daugherty. *Training Cyber Warriors: What Can Be Learned from Defense Language Training?* Santa Monica, CA: RAND Corporation, 2015.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.

_____. *Cyberdeterrence and Cyberwar*. RAND Corporation Monograph Series. Santa Monica, CA: RAND, 2009.

_____. *Defending Cyberspace, and Other Metaphors*. Washington, DC: National Defense University, 1997.

_____. *Cyberspace in Peace and War*: *Transforming War*. Annapolis, MD: Naval Institute Press, 2016.

_____. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND, 2012.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press, 2015.

Looking Glass. *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare*. Lookingglass Cyber Threat Intelligence Group, CTIG-20150428-01, April 28, 2015. Accessed October 30, 2017. https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf.

Medvedev, Sergei A. "Offense-defense theory analysis of Russian cyber capability." Monograph, Naval Postgraduate School, 2015. Accessed November 16, 2017. https://calhoun.nps.edu /bitstream/handle/10945/45225/15Mar_Medvedev_Sergei. pdf;sequence=3.

Miller, Donald L. *D-Days in the Pacific*. New York: Simon & Schuster, 2005.

Monaghan, Andrew. "Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare.' *Parameters* 45, no. 4 (Winter 2015-16): 65-74. Accessed October 30, 2017. http://ssi.armywar college.edu/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf.

Mueller, Joseph N. *Osprey Campaign Series*. Vol. 18, *Guadalcanal 1942: The Marines Strike Back*. London: Osprey, 1992.

Nebeker, Frederik. *Dawn of the Electronic Age: Electrical Technologies in the Shaping of the Modern World, 1914 to 1945*. Piscataway, NJ: IEEE, 2009.

Naveh, Shimon. *The Cummings Center Series*. Vol. 7, *In Pursuit of Military Excellence: The Evolution of Operational Theory*. London: Frank Cass, 1997.

Olsen, John Andreas, ed. *The Evolution of Operational Art: From Napoleon to the Present*. Oxford: Oxford University Press, 2011.

Perkins, David. "Multi-Domain Battle: Driving Change to Win in the Future." *Military Review* (July-August 2017): 6-12.

Peterson, Nolan. "How Russia's Cyberattacks Have Affected Ukraine." Last modified December 16, 2016. Accessed October 30, 2017. http://dailysignal.com/2016/12/16/how-russias-cyberattacks-have-affected-ukraine/.

Swain, Richard M. "Filling the Void: The Operational Art and the U.S. Army." In *Operational Art: Developments in the Theory of War*, 147-172, edited by B.J.B. McKercher and Michael Hennessey, 147-172. Westport, CT: Praeger, 1996. Accessed August 11, 2017. https://cgsc.blackboard.com/webapps/blackboard/execute/content/file?cmd=view&content_id=_540319_1&course_id=_7174_1.

Svechin, Aleksandr. *Strategy*. Edited by Kent D. Lee. Minneapolis, MN: East View Publications, 1992. Original printing 1927.

Schneider, James J. *Vulcan's Anvil: The American Civil War and the Foundations of Operational Art, Theoretical Paper No. Four*. Fort Leavenworth, KS: School of Advanced Military Studies, Command and General Staff College, 1992.

Snegovaya, Maria. “Russia Report I: Putin’s Information Warfare in Ukraine.” Institute for the Study of Warfare, September 2015. Accessed October 30, 2017. http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Stinissen, Jan. “A Legal Framework for Cyber Operations in Ukraine.” In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 123-134. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015. Accessed November 9, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf.

The Institute for National Security Studies (INSS). “The Ukrainian crisis- a cyber warfare battlefield.” *Defense Update*, April 5, 2014. Accessed November 16, 2017. http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html.

Thompson, Charles E. “Miracle on the Vistula: The Red Army’s Failure and the Birth of the Deep Operations Theory of Annihilation.” Monograph, School of Advanced Military Studies, US Army CGSC, 2018.

Thomas, Timothy L. *Decoding the Virtual Dragon.* Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

_____. *Dragon Bytes: Chinese Information-War Theory and Practice*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

_____. *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics.* Fort Leavenworth, KS: Foreign Military Studies Office, 2015.

_____. *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker*. Fort Leavenworth, KS: Foreign Military Studies Office, 2012.

_____. *Kremlin Kontrol: Russia’s Political-Military Reality*. Fort Leavenworth, KS: Foreign Military Studies Office, 2017.

US Department of the Army. Army Doctrinal Publication 3-0, *Operations*. Washington, DC: Government Printing Office, 2016.

_____. Army Doctrinal Reference Publication 3-0, *Operations*. Washington, DC: Government Printing Office, 2016.

_____. Army Doctrinal Reference Publication 3-90, *Offense and Defense*. Washington, DC: Government Printing Office, 2012.

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

US Department of Defense. Joint Staff. Joint Publication 3-0, *Joint Operations*, Washington, DC: Government Printing Office, 2017.

_____. Joint Staff. Joint Publication 5-0, *Joint Planning*, Washington, DC: Government Printing Office, 2017.

_____. Joint Staff. Joint Publication 3-12 (R), *Cyberspace Operations*, Washington, DC: Government Printing Office, 2013.

_____. Joint Operational Access Concept, Version 1.0. Washington, DC: United States Department of Defense, 2012. Accessed August 19, 2017. https://www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf.

US Joint Staff Joint Force Development (J7)- Future Joint Force Development. *Cross-Domain Synergy in Joint Operations, Planner's guide*, January 14, 2016. Accessed August 19, 2017. http://www.dtic.mil/doctrine/concepts/joint_concepts/cross_domain_planning_guide.pdf.

US Army Training and Doctrine Command. White Paper. "Multi-Domain Battle: Combined Arms for the 21st Century," February 24, 2017. Accessed July 19, 2017. http://www.tradoc.army.mil/multidomainbattle/docs/MDB_WhitePaper.pdf.

USSR. Military Affairs, *Provisional Field Regulations for the Red Army, Vremennyy Polevoy Ustav, RKKA 1936 (PU 36)* original in Russian, 1937. Foreign Broadcast Information Service, June 12, 1986. Accessed November 1, 2017. handle.dtic.mil/100.2/ADA361873.

Weedon, Jen. "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 67-77. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015. Accessed November 9, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/cyberwarinperspective_full_book.pdf

Weedon, Jen, and Laura Galante. "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast." FireEye Executive Perspectives, March 12, 2014. Accessed November 13, 2017. https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russiahackers-cyberwar-not-so-fast.html.