Cyberwarfare and Operational Art

A Monograph

by

MAJ Timothy J. Williams
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
21-02-2017	Master's Thesis	JUN 2016 – MAY 2017

4. TITLE AND SUBTITLE
Cyberwarfare and Operational Art

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Timothy J Williams, 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 ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Operational Arts Studies Fellowship, 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
International actors engage in cyber warfare to include the People's Republic of China, the Democratic People's Republic of North Korea, the Islamic Republic of Iran, and non-state actors. Cyber warfare evolved into synchronized activities to achieve strategic objectives. This research asserts that the characteristics of cyberspace amplify the aspects of cross-domain warfare within the framework of operational art. The case study evaluated the Russian Federation cyber operations in time and space to support a theory that cyber and land force actions can transform mutual operational reach. Further, the study employed modeling of observed interactions which indicate synchronous land and cyber power change the construct of the operational art regarding tempo to transform the time, space and purpose for strategic aims. The study provides a conceptual framework to aid in answering the following questions. First, how do military forces protect against an adversary with sophisticated cyber warfare and cyber intelligence, surveillance, and reconnaissance (ISR) capabilities? Second, how can the US Army can best integrate Cyber Support to Corps and Below (CSCB) to close the strategic-to-tactical cyber gap?

15. SUBJECT TERMS
Cyberwarfare, cyber-joint operations, Russo-Ukrainian conflict, Cyber Support to Corps and Below (CSCB)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Major Timothy J Williams
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified		50	912-271-6274

Monograph Approval Page

Name of Candidate: Major Timothy J. Williams

Monograph Title: Cyberspace and Operational Art

Approved by:

_____, Monograph Director
Bruce E. Stanley, PhD

_____, Seminar Leader
G. T. Puntney, Lt Col

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

Accepted this 25th day of May 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

Abstract

Cyberwarfare and Operational Art, by MAJ Timothy J. Williams, US Army, 49 pages

International actors engage in cyber warfare to include the Russian Federation, the People's Republic of China, the Democratic People's Republic of North Korea, the Islamic Republic of Iran, and non-state actors. Cyber warfare evolved into synchronized activities to achieve strategic objectives. This research asserts that the characteristics of cyberspace amplify the aspects of cross-domain warfare within the framework of operational art. The case study evaluated the Russian Federation cyber operations in time and space to support a theory that cyber and land force actions can transform mutual operational reach. Further, the study employed modeling of observed interactions which indicate synchronous land and cyber power change the construct of the operational art regarding tempo to transform the time, space and purpose for strategic aims. The study provides a conceptual framework to aid in answering the following questions. First, how do military forces protect against an adversary with sophisticated cyber warfare and cyber intelligence, surveillance, and reconnaissance (ISR) capabilities? Second, how can the US Army can best integrate Cyber Support to Corps and Below (CSCB) to close the strategic-to-tactical cyber gap?

Contents

Acknowledgement

As all military families, the Williams family has given its all and sacrificed to support the United States Army and myself for twelve years. My wife, Kimberley and Aaron, my son, gave up the time with me our last few years for the service and the research. We hope our contribution significantly provided toward the understanding and answered the illusive questions hidden in this body of study. Thank you Williams clan, I love you both.

My heroes: Dr. Bruce Stanley, Lt Col Todd Puntney, Colonel (R) Peter Im have supported my wild spirit of discovery but more importantly, my personal development. Each of you are a mentor whom I cherish for input and guidance. Likewise, Brigadier General Willard Burleson III and Lieutenant Colonel Jim Browning instilled a passion for our profession and cyber warfare. You all set me along the path toward the School of Advanced Military Studies, thank you gentlemen. Climb to Glory!

My peers and friends. Specifically, Majors Joe DiDomenico, Chad Corbin, Tennille Scott, Ryan Hand, and Brian Walker; all of you have provided incredible input and peer development to this study and my professional development as an officer. In the Shadows.

Finally, my mentees: You gentlemen represent the Army's future. Tony and Josh, do your best, serve your country, always care for your family. Above all revere your purpose placed for you by God.

Acronyms

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
ARPANET	Advanced Research Projects Agency Network
BTC	Baku, Tbilisi, Ceyhan (British Petroleum owned oil pipeline)
CENTCOM	Central Command
CGSC	Command and General Staff College
CNA	Computer Network Attack
CSCB	Cyber Support to Corps and Below
EA	Electronic Attack
EMS	Electro Magnetic Spectrum
FM	Field Manual
FSB	Federal Security Service (Russian Federation)
GAO	General Accounting Office
GRU	Military Intelligence Directorate (Russian Federation)
IoT	Internet of Things
ISR	Intelligence, Surveillance, and Reconnaissance
ISP	Internet Service Provider
IXP	Internet Exchange Point
JOAC	Joint Operational Access Concept
JP	Joint Publication
KSO	Special Operations Command (Russian Federation)
NATO	North Atlantic Treaty Organization
NCW	Net-Centric Warfare
NGW	New-Generation Warfare
OCO	Offensive Cyber Operations
OODA	Orient, Observe, Decide, Act

opSpN	Independent Special Purpose Regiment (Russian Federation Spetsnaz)
OSC	Offensive Space Control
PC	Personal Computer
RFC	Request for Comment
RMS	Remote Manipulator Systems
RAT	Remote Access Tool
SAMS	School of Advanced Military Studies
SCADA	Supervisory Control and Data Access
SIGINT	Signals Intelligence
TCP/IP	Transmission Control Protocol/Internet Protocol
TTP	Tactics, Techniques, and Procedures
VDV	Russian Airborne Troops
W3C	World Wide Web Consortium

Illustrations

Introduction

> An important feature of a learning machine is that its teacher will often be very largely ignorant of quite what is going on inside, although he may still be able to some extent to predict his pupil's behavior.
>
> —Alan M. Turing, “Computing Machinery and Intelligence”

Jeffrey Carr, a cyber intelligence expert and founder of Taia Global, observes that the complexity and secrecy of cyberspace have confounded the thinking of senior national security leadership.[1] Cyberspace manifested on March 18, 1940, when Alan Turing developed the "electromechanical mind." Turing along with others at Bletchley Park, United Kingdom built the cyber-mind to decrypt the communications within “Enigma,” “Fish,” and “Magic” that connected the Axis Powers’ through a global electromagnetic communications network.[2] Cyberpower emerged from these counter-cryptographic operations of World War II and evolved, with the advent of the United States’ Advanced Research Projects Agency Network (ARPANET), into a global

[1] “The limited thinking of senior leadership…[regarding] how attacks orchestrated by a myriad of parties across the globally connected networks are impacting national security for the United States and other nation-states, we’re all like blind men describing an elephant.” Jeffery Carr, *Inside Cyber Warfare,* (Cambridge, MA: O’Reilly Media Inc., 2012), 74.

[2] "The Bombe developed in Bletchley by Turing and Welshman and Babbage - all luminaries of the Cambridge scene[.]…And it was because of the greater difficulties of dealing with the Enigma that it had to be that powerful… [I]n particular it [the decryption] would be impossible because each of the Enigma and the Fish were used by the Germans as the basis not merely for one cipher each, not merely one Enigma and one Fish, but as the basis for a wide range of different ciphers, each cipher having its different key... [In regard to ULTRA distribution and intercept of electromagnetic communications,] except for the Atlantic traffic the American coast couldn't intercept European, German and Italian signals. That was all being intercepted in the UK. Obvious solution - UK concentrates on decrypting, on cryptanalysis against German and Italian. America which can intercept the Pacific from the Pacific and also has headquarters in Brisbane and various places in the Pacific - America concentrates on working on the Japanese." Sir Harry Hinsley, "The Influence of ULTRA in the Second World War," (lecture, Security Group Seminar, Babbage Lecture Theater Computer Laboratory, Cambridge University, Cambridge, November 26, 1996).

network to survive nuclear holocaust during the Cold War.[3] ARPANET's design became the framework of modern cyberspace that has been embedded to control human space.[4]

ARPANET's survivable structure provided the means for cyber war to go beyond signals and technical intelligence within the framework that became the Internet. By the 1980s, the first documented cases of cyberattacks against infrastructure, economies, and intellectual property had begun to appear.[5] By the twenty-first century, the Russian Federation enhanced offensive attacks through cyberspace against Georgia in 2008 and later synthesized cyber and land power during the invasion of Ukraine in 2014.[6] The second decade of the twenty-first century has witnessed multiple nation-states engage in cyber warfare including the People's Republic of China, the Democratic People's Republic of North Korea, the Islamic Republic of Iran, and non-state actors.[7] Cyber warfare evolved into synchronized activities to achieve strategic objectives. This research asserts that the characteristics of cyberspace amplify the aspects of cross-domain warfare within the framework of operational art.

The significance of this research provides an initial contribution to the theory and understanding of cyberspace and the general theory of warfare. The study provides a conceptual framework to aid in answering the following questions. First, how do military forces protect against

---

[3] Leonard Kleinrock et al., "Computer Network Research," *Advanced Research Projects Agency Semiannual Technical Report* (Los Angeles: University of California, June 30, 1972): 1-7. Computer Network research documented in the January 1 to June 30, 1972, marked the beginning studies in the optimization of large computer networks and is universally recognized as the start of the Internet. Further, the technical specifications and control structure developed through ARPANET began the standard of global networks that became the internet and all classical network protocol structures.

[4] Farouk Kamoun et al., "Hierarchical Routing Procedures for Large Computing Networks," *Design Considerations for Large Computer Communication Networks, ARPA CONTRACT No DAHC-15-73-C-0368* (Los Angeles: School of Engineering and Applied Sciences, University of California, April, 1976): 12-24.

[5] The Economist, "Cyberwar: War in the fifth domain," *The Economist: Brief,* last modified July 1, 2010, accessed August 17, 2016, http://www.economist.com/node/16478792; Carr, *Inside Cyber Warfare,* 14.

[6] Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, art 7 (2015): 1-2; Carr, *Inside Cyber Warfare,* 12-14.

[7] Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins, 2010), 189-195; Carr, *Inside Cyber Warfare,* 2-4 & 243-258.

an adversary with sophisticated cyber warfare and cyber intelligence, surveillance, and reconnaissance (ISR) capabilities? Second, how can the US Army can best integrate Cyber Support to Corps and Below (CSCB) to close the strategic-to-tactical cyber gap?[8]

These questions require contextual familiarity with cyberspace, operational art, operational reach, operational tempo, and cross domain warfare. Richard Clarke, who served as the National Coordinator for Security, Infrastructure Protection, and Counterterrorism provides a classic definition of cyberspace that reflects the Joint definition of Cyber Operations. Clarke defines cyberspace as a global domain of "all the computer networks in the world and everything they connect and control."[9] Operational art, as a cognitive approach to planning, is the synchronization of actions in time, space, and purpose to achieve strategic objectives.[10] Joint Doctrine defines operational reach as "the distance and duration across which a joint force can successfully employ military capabilities."[11] The concept of operational tempo defined by Robert R. Leonhard expands beyond the notion of the velocity of events. Leonhard defines operational tempo as the frequency, duration, and sequencing of events (and tactical engagements).[12] Former Chairman of the Joint Chiefs of Staff Martin Dempsey defined cross-domain warfare in the Joint Operational Access

---

[8] Brigadier General John S. Kem to The Army University, August 15, 2016. "Topics for Consideration by SAMS, CGSC and Other Students for MMAS and Other Degree Program/Requirements" (Fort Leavenworth: US Command and General Staff College, 2016), 11.

[9] Clarke and Knake, *Cyber War*, 70*;* "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Publication (JP) 3-12 Redacted (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 2013), GL-4.

[10] Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process* (Washington, DC: Government Printing Office, 2012), 2-1, 2-2.

[11] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, August 11, 2011), III-28.

[12] Robert R. Leonhard, *Fighting by Minutes: Time and the Art of War* (Westport, CT: Praeger, 1994), 10-11.

Concept as "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others—to establish superiority in some combination of domains that will provide the freedom of action required by the mission."[13] General Dempsey extends this definition beyond that of multi-domain warfare, which is the simultaneous strategic effect of domains without regard to the interdependent nature of operational approaches in each domain.

General Dempsey recognized that the resonance between domains of warfare depends on their interaction of behaviors and capabilities within the context of operational outcomes. Theoretically, planners may employ these interactions to exploit systemic domain advantages. The associated interactions between cyberspace and cross-domain warfare must be understood to form optimal options for commanders. An understanding of this resonance in warfare leads to choices and opportunities. For example, Figure 1.1 models the theoretical interaction of cyber and land operations which produces a vastly different potential outcome with segregated activities regarding the tempo and operational reach.

The research relies on two hypotheses. First, if land operations alter the state of cyberspace, then land power (or other domains) must be synchronized with cyber operations for operational reach. Second, if cyber operations impact landpower, then cyberspace may alter the available time, space and purpose of land warfare. Two focused questions were used to gather the empirical evidence to test the hypotheses. First, how do the characteristics of cyberspace operations affect the aspects of operational reach? Second, how can a synchronization of anticipated characteristics of cyberspace impact joint tempo? The research potentially provides a cognitive framework of operational art that conjoins cyber operations with the other domains in the joint context.

---

[13] General Martin E. Dempsey, "Forward," *Joint Operational Access Concept (JOAC) v 1.0* (Washington, DC: Government Printing Office, 2012).

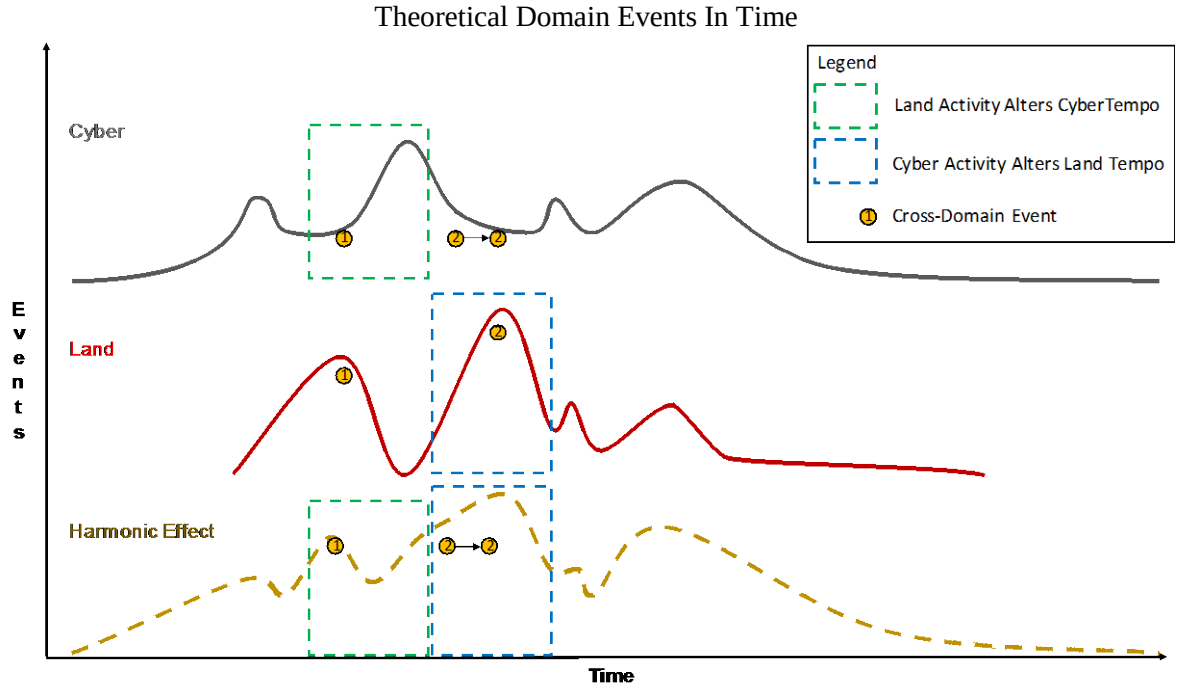

Figure 1.1. Single to Cross-Domain Effects. (1) Land action alters cyberspace enabling continued cyber activities. (2) Sustained cyber activities enable effectiveness of land domain. The expected cyber and land interactions with amplified (harmonic) effects.

The research material focused on only unclassified publicly known actions attributable to the Russian Federation between March 2013 and January 2015 within the territory of the Ukraine. The primary purpose of analysis centered on the interaction of cyberpower and landpower. This study does not consider international implications of law and policy level decisions, nor did the research explore the consequences of attacks on "complex systems engineering."[14] This paper applied the American interpretation of “reflexive control” for analysis of Russian application of cyber power.[15] The paper attempted to frame a complex system to conceptualize the interaction of cyberspace and provide greater clarity for understanding cross-domain warfare.

---

[14] Douglas O. Norman and Michael L. Kuras, “Engineering Complex Systems,” *Selected Readings D300: Army Design Methodology AY 2011-12* (Fort Leavenworth: School of Advanced Military Studies, 2011):16-7.

[15] Maria Snegovaya, “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare,” *Russia Report* 1 (Washington, DC: Institute for the Study of War, September 2015), 7.

Four assumptions guided the theoretical basis for research. First, hacker culture imposes a degree of internal social context concerning the conduct of cyberspace activities.[16] Second, regardless of multiple purposes for synchronization of cyber operations with land formations, the Russian Federation campaign evolved its operational approach from a theory of "deep battle" during multiple decades before 2013.[17] Third, the open source offensive cyber tools attributed to the analyzed campaign have been adequately quantified and led to the success of the main events within the case study. Finally, the reduction to land, space and cyber does not obfuscate the overall interactions of other natural domains.

The study is organized into six sections: the introduction, literature review, methodology, case study, findings, and conclusion. The literature review builds a theoretical and conceptual context of operational art and cyberspace which connects to the contextual model of cyberspace relative to the other domains of warfare for further analysis. Next, the methodology provides a framework of the structured focused approach to assess cyberspace's characteristics and apply operational art for an established process. The findings section synthesizes the evidence of the case study within the theoretical hypothesizes. The conclusion draws from the findings to recommend an application of cyberpower within joint operations.

---

[16] "1. A person who delights in having an intimate understanding of the inner workings of a system, computers and computer networks in particular. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming." G. Malkin, "Internet Users' Glossary," network Working Group, *Request for Comments: 1122 (RFC 1122)* (Network Working Group, Internet Engineering Task Force, October 1989) ed. R. Braden, accessed July 29, 2016, https://tools.ietf.org/html/rfc1122#section-1.1.2.; "[The question is:] The best way to promote this free exchange of information is to have an open system, something that presents no boundaries between hacker and a piece of information or an item of equipment…[When] bureaucracies, whether corporate, government, or university, are flawed systems, dangerous in that they cannot accommodate the exploratory impulse of true hackers." Steven Levy, *hackers: heroes of the computer revolution* (Sebastopol, California: O'Reilly, 2010), 29. RFC1392 provided the definitions for understanding cyberspace. RFCs provide the collaborative framework in which all internet terms, references, design, and implementation are based. In military terms, an RFC is the doctrinal and capability implementation of cyberspace. The assumptions are thus that hacker culture imposed a humanist character to the physics of the cyber environment.

[17] Carr, *Inside Cyber Warfare,* 161-71.

Literature Review

A groundwork to support the theory of cyberspace is necessary to provide military practitioners an asymmetric means over other domains of warfare. Operational art framed within the context of Russian deep battle theory and academic models of joint cyber-land operations provides a structured focused approach to assessing the Russo-Ukrainian conflict.

A theoretical model of operational art provides a cognitive framework to seize success in modern warfare. SAMS founder, Brigadier General Huba Wass De Czege, described operational art as the genius to apply tactical actions toward strategic ends in time, space, and purpose.[18] Russian operational art adapted deep battle to solve the obstacles of early post-World War I breakout. Professor Robert Citino observed through researching interwar German military scholarship that Prussian General von Moltke the Elder influenced Russian theories as a contest toward the objective in both time and space.[19] Naveh described the Russian theorist Tukhachevsky's ideas had substituted destruction '*Verichtung*' of armies with the concept of operational shock '*udar'* that leads to the annihilation of the enemies' war systems by the race of time.[20] Both 20th century German and Russian operational theories link the Prussian theories of Clausewitz and Moltke the Elder to the problem environment observed by Georgii Samoilovich Isserson which could overcome friction by the use of time to dominate command and control.

---

[18] Huba Wass de Czege, "Thinking and Acting Like an Early Explorer: Operational Art is not a Level of War," *Small Wars Journal*, last modified March 14, 2011, accessed August 12, 2016, http://www.smallwarsjournal.com/blog/journal/docs-temp/719-deczege, 6.

[19] Robert Citino, "'*Die Gedanken Sind Frei*': The Intellectual Culture of the Interwar German Army," *The Army Doctrine and Training Bulletin* 4, no. 3 (Fall 2001), 50-1.

[20] William J. Mc Granahan, "The Fall and Rise of Marshal Tukhachevsky," *Parameters* 8, no. 4 (1978): 68-69; Shimon Naveh, *In Pursuit of Military Excellence*, 11. Tukachevsky as interpreted by 'annihilation' which he implored as the military end state and Naveh post-edited as a strategic end, annihilation.

Isserson provided a model of the mechanism for military formation and function: deep battle. He proposed composing sequences of actions in time and into the depths of enemy spaces.[21] Russian theorists such as Isserson adapted Tukhachevskii's theories to include the elements of operational maneuver such as "fragmented strike," simultaneity, and momentum to achieve "multi-level battle waged on several tiers within the operational depths."[22] The Russians, according to Naveh, analyzed and applied the operational qualities of each combat unit regarding mobility, firepower, and protection to optimize form for function.

The Russians then balanced combinations of operational capabilities of each combined arms unit within each strike force based off of the predicted operational circumstances.[23] Tukhachevskii states that deep battle applies:

> "[T]he power of the combined arms strike [*obschevoiskovogo udara*] with the successive movements by bounds and the breakout into the area whose seizure signifies the annihilation and defeat of the enemy. Synergetic command and control must then ensure synchronization between the forces involved at all stages of fighting."[24]

The Russian deep battle theory sought to employ shaped organizations for the singular purpose to break through the enemy and strike the deployment, mobility, and command centers behind forward lines before the opponent could counteract; to race toward the time a unit cohesively maintains its systems. (Figure 2.1).

---

[21] Carl Von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 209; Naveh, *In Pursuit of Military Excellence*, 33.

[22] Georgii Samoilovich Isserson, *The Evolution of Operational Art*, translated by Bruce W. Menning (Fort Leavenworth: Combat Studies Institute Press, 2013), 67-8.

[23] Azar Gat, *A History of Military Thought: From the Enlightenment to the Cold War* (New York: Oxford University Press, 2001), *637*; Naveh, *In Pursuit of Military Excellence*, 226, 233.

[24] M.N. Tukhachevskii, "New Issues of War: Новые вопросы войны," *Voenno-Istoicheskii Zhurnal, no. 2* (1962): 73-5 quoted in Naveh, *In Pursuit of Military Excellence*, 234-235.

The Russian Deep Battle Theory (1938)

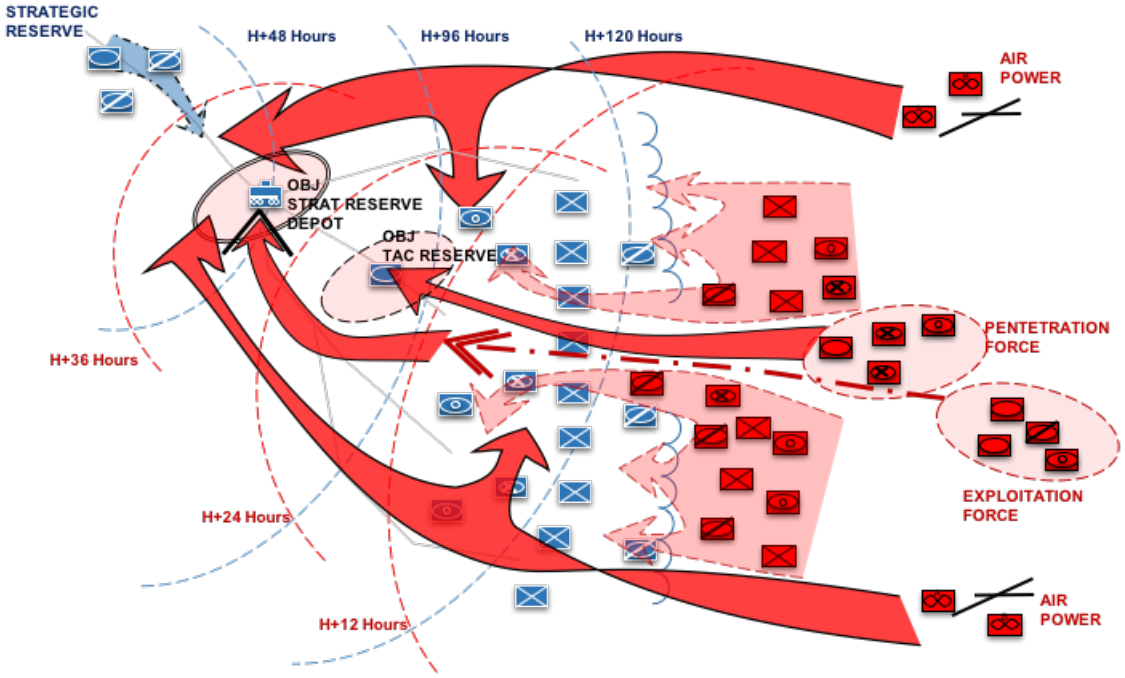

Figure 2.1. Deep Battle. Separate operational tempos of land; the race to the Blue Force strategic deployment area (STRAT RESERVE DEPOT). Source Richard W. Harrison, *Architect of Soviet Victory in World War II* (Jefferson, NC: McFarland & Company, 2010), 114.

The United States military adopted operational art as a transformative concept after 1978. The American military codified operational art as a cognitive function to operationalize national means and achieve political ends to counter Soviet deep battle doctrine. Similar to the Russian theory, American operational art became a cognitive approach to alter opposed systems by attacking decisive points through a synchronization across the temporal depth of the battle area.[25]

Global cyber warfare potentially provides an extradimensional means that complements deep battle and amplifies immediate land warfare. The cyberspace domain came into being from the scientific research to resolve solutions to complex problems, such as breaking the Enigma

[25] Antulio J. Echevarria II, "American Operational Art, 1917-2008," *Evolution of Operational Art*, edited by John Andreas Olsen and Martin Van Creveld (New York: Oxford University Press, 2011), 154-55; "Operational art is the use of creative thinking by commanders and staffs to design strategies, campaigns, and major operations and organize and employ military forces." JP 3-0, *Joint Operations*, xii.

cryptography or surviving holocaust. Alan Turing hypothesized that the engineers of the military global intelligence apparatus would not be able to understand the logic to which it operated.[26] For instance, the makers of the United States' ARPANET could not foresee the global implications of control or cognitive spaces their system would create.[27] Thus the architects of the new synthetic human domain had no means of understanding the consequence of the complex open system that they had designed.

The open system evolved from hackers in elite clubs at engineering universities to plan digitized assaults between nation-states. The 1970s hackers evolved the Alan Turing cybernetic-apocrypha into the modern technology that became personal computers (PCs), Supervisory Control and Data Acquisition (SCADA) networks, video games, virtual reality, iPhones, and the internet of things (IoT).[28] Hacking and the derivative actions facilitated electronic and computer network attack (EA and CNA); tactical engagements with the purpose of altering systems. Military practitioners adopted the hacker mentality and methods that weaponized human innovation.

The effects of cybernetic manipulations mirrored military operational art to exploit enemy weaknesses and gain temporal dominance.[29] As Antoine Bousquet realized, mechanistic warfare

---

[26] Turing, "Computing Machinery and Intelligence," *Mind New Series* 59, no. 236 (October 1950): 437-9, 448-9; M.D. Godfrey and D.F. Hendry, "The Computer as von Neumann Planned It," *IEEE Annals of the History of Computing* 15, *no. 1* (1993): 11. The 'Imitation Game' logically extends to consider the creation of the electromechanical mind toward the evolved networked digital computer system as a thinking machine system, a complex adaptive system, that exceeds the cognitive understanding of those who brought the new intelligence into existence.

[27] Leonard Kleinrock et al., "Computer Network Research," *Advanced Research Projects Agency Semiannual Technical Report* (Los Angeles: University of California, December 31, 1973), 3-4; Kleinrock, "Computer Network Research," *(1972),* 3. The reports detail that the progression of specifications for ARPANET and the integration of space telecommunication systems. However, the reports in 1973 begin to describe the process of system security as an endless task.

[28] Levy, *hackers*, 79, 255, 329. The "Third Generation" hackers altered Atari's closed system architecture, executed communication frauds, and also created new personal computer technologies that established Apple Corporation: Steve Wozniak. The third generation movement became the innovators of 1980s and 90s.

[29] Everett Carl Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Routledge, 2005), 152-3. Dolman connects the conservation of time to the tactical engagements that achieve control of tempo and the prediction of these acts by strategy. Operational art seeks to adapt to

became systems synchronized by autonomous parts. Twentieth century commanders struggled to maintain control and prevent their opponents from attacking their systems.[30] The United States defense theorists developed the doctrine of Network-Centric Warfare (NCW) to employ the advantages of defensive cyber power.[31] Between 1990 to 2005, early information age theorists framed cyber power as sharing knowledge across all networked nodes rapidly to outpace adversary decision cycles and seize an asymmetric advantage.

The NCW theory ignored the counter threat of cyberpower which could attack its functions. The net-centric and net-war conceptualization of cyber power employed the idea of rapid-complete situational awareness and action.[32] John Arquilla's description of the employment of cyber capabilities by various non-state actors proposed a concept for net-war which complements Libicki's, the lead theorist of NCW, information warfare vision of cyber power.[33] However, these theories evangelize flawed asymmetric advantages predicated on NCW's asymmetric benefits while exposing cohesive systems to cyber-attack. Cyber reliance expands the cyber-surface area that opponents could assault into cognitive and physical space provided from advanced microprocessor enhanced systems interconnectivity.

Cyberspace operates from a standardized network system architecture which provides simple approaches to overcome complex problem sets. The Transmission Control Protocol/Internet

---

emerging situations continually. Dolman links his ideas to Boyd's OODA loop as an attempt to achieve this goal.

[30] Antoine Bousquet, *The Scientific War of Warfare: Order and Chaos on Battlefields of Modernity* (New York: Columbia University Press, 2009), 31.

[31] Bousquet, *The Scientific War of Warfare*, 35.

[32] Colin S. Gray, "Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling," *Strategic Studies Institute Monograph* (April, 2013): 45; A. K. Cebrowski, *Implementation of Net-Centric Warfare* (Washington, DC: Office of Force Transformation, January 5, 2005), 15.

[33] National Defense Research Institute, *Networks, and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Washington, DC: National Defense Research Institute, 2001), 2; Martin C. Libicki, *What Is Information Warfare* (Washington, DC: US Government Printing Office, August, 1995), 7-8.

Protocol (TCP/IP) model implemented by the Internet Engineering Task Force, Request For Comment 1122 (RFC 1122) in 1989 evolved concepts of cyberspace to establish a "good practice" globally. The open source, globally understood, TCP/IP system provides optimal routing services for legitimate use. However, the same norms of "good practice" generate attack surfaces for hackers. Cyberspace's transmutable interactions imposed by collective engineering agreements created operational gaps through simplicity. Hackers could alter the rules of logical cyberspace and manipulate the relative characteristics of time and space across domains. The malleability of the TCP/IP architecture, computer code, functions, and even hardware "states" allow the operating laws to be transformed for divergent purposes.

Cyberspace after 1991 provided an immense environment for hackers to exploit the engineered laws of cyberspace.[34] Practitioners and executives discounted the legal perils of manipulation in the 1990s as security issues to litigate hackers in Western states.[35] Instead, the art of hacking became a criminal sub-culture within the United States. Hacker persecution supported the interests of Cold Warriors protecting the legacy of ULTRA and ARPANET.[36] Simultaneously, the twenty-first century experienced the information revolution that expanded cyberspace across virtual sovereign territories. Cyber security firm Symantec implicated the Stuxnet creators as a nation-state that employed over thirteen hacker tactics, techniques, and procedures (TTPs) which destroyed the strategic Iranian nuclear reactors at Natanz.[37] The Russian Federation and the

---

[34] Berners-Lee, Tim. "The Original HTTP as defined in 1991" (World Wide Web Consortium (W3C), 1991), accessed September 01, 2016, http://www.w3.org/Protocols/HTTP/AsImplemented.html.

[35] Network Working Group, *Request for Comments: 1122 (RFC 1122),* https://tools.ietf.org/html/rfc1122#section-1.1.2.

[36] Richard Stallman, "The Hacker Community and Ethics: An Interview with Richard M. Stallman, 2002," *Tere Vade,* (Tempere, Finland: Tampere University Press, 2002).

[37] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier: Version 1.4," *Symantec Security Response Report* (February, 2011): 2.

People's Republic of China supported hacker savants to their advantages. Meanwhile cyberspace provided a global means to control populations, industry, media, and ultimately institutions of reality.[38] Cyberspace exploded as a world of blind users, rebellious hackers, and professionalized cyber-authoritarians.

Fred Schreier's DCAF Horizon 2015 Working Paper best summarizes cyberspace domain's fundamental characteristics. First, cyberspace requires the Electro Magnetic Spectrum (EMS) to propagate efficiently. Second, cyberspace needs man-made physical objects to generate nodes within its topography.[39] Third, human actions transform cyberspace constantly. Fourth, cyberspace's barriers to entry decrease rapidly relative to Moore's Law.[40] Fifth, offense rather than defense is the dominant form of warfare in cyberspace.[41] Finally, cyber warfare is not information warfare but warfare within a domain that can significantly impact all the physical domains and control environments including that of information.[42]

Cyber operations require a set of domain characteristics to establish a basis for analysis. The following conceptual framework merges the cyber warfare findings of Schreier and Liles with

---

[38] US Department of Defense, *The Department of Defense Cyber Strategy*, (Washington DC: Office of the Secretary of Defense, April 2013), 1-2; David S. Alberts and Richard E. Hayes, *Power to the Edge* (Washington, DC: DoD Command and Control Research Program, June 2003), 90-3.

[39] Samuel Liles et al., "Applying Traditional Military Principles to Cyber Warfare," *2012 4th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCD COE Publication, 2012), 172-4.

[40] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (April 19, 1965). Moore's law states that each year the number of transistors in a fabricated dye will double. The information technology sector has observed the same relative exponential growth in processor rates for the last three decades.

[41] Fred Schreier, "On Cyberwarfare," *DCAF Horizon 2015 Working Paper*, no. 7 (Geneva, Switzerland: Geneva Centre for Democratic Control of Armed Forces, 2015): 12-3.

[42] "The logical network layer is the first point where the connection to the physical dimension of the information environment is lost." Joint Publication (JP) 3-12, *Cyber Operations* (Washington, DC: Government Printing Office, February 5, 2013), IV-3; "On Cyberwarfare," 24. The human information space and the physical connections of cyberspace did not collocate in the natural world but delimited through the logical layer of cyberspace. Therefore, cyberspace has been made to transmit as a medium the human modality of information but is not controlled by the information constructs.

other domain theorists, Mahan, Corbett, Mitchell, and Klein, to propose the fundamental characteristics of cyberwarfare.[43]

Cyber power evolved to include two of sea power's principles: defense of safe ports to ensure commerce and the connection of lines of communication to land forces by way of the sea domain. Mahan's stress on the defense and communications from remote ports provides the strength to the fleet.[44] Mahan describes the sea domain as a vast commons, "which men may pass in all directions, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others."[45] Also, Mahan postulates that "The character of its harbors that are to be considered."[46] Corbett connects the relationship of the maritime fleet to protecting against the enemy fleet providing "covering" support to the land operations. He theoretically linked sea and land operations as essential for strategic success.[47] Cyberspace relies on the physical nodes that conceptually interconnect from the physical infrastructure.

Cyber power compliments the conceptual ideas of air power writers and provides two more concepts previously unique from the air domain of warfare: indirectly opposing air forces cannot win air power, and air supremacy enables the operational reach of air power. Giulio Douhet philosophized that instead of the mass slaughter seen during the Great War; the application of absolute war rapidly imposes on the opposing force through air power would prove decisive. Douhet's key is found in his eight fundamental principles of air power, but one is critical to cyber

---

[43] Schreier, "On Cyberwarfare," 12-3; Liles, "Applying Traditional Military Principles to Cyber Warfare," 172-4.

[44] A. T. Mahan, *The Influence of Sea Power Upon History 1660-1783* (New York: Dover Publications Inc., 1987), 83.

[45] Mahan, *The Influence of Sea Power*, 25.

[46] Mahan, *The Influence of Sea Power*, 43.

[47] Julian S. Corbett, *Principles of Maritime Strategy* (Mineola, NY: Dover Publications, 2004), 290-1; Gat, *A History of Military Thought*, 486-87.

power: the priority is the command of the air by countering opposing air forces.[48] Ultimately, cyber power leverages Douhet's concepts of strategic bombing, immediate air supremacy with those of Billy Mitchell for the operational reach of air power versus strategic outcomes. Cyber power, like air power, must gain temporal dominance in the cyber domain.[49]

While space power does not have an operational theory or artist connected to it, the domain does have principles that can contribute to the understanding of cyberspace. Space power like air and sea power requires the use of choke points or hubs of activity. However, unlike air and sea, space relies on satellites in discreet orbits controlled by air, sea, or land infrastructure to maintain advantageous positions.[50] Next, the orbits of space power like the sea lines of communication provide equal utility to all nations and highly sought after connections in cyber power.[51] Joint Publication 3-14, *Space Operations,* describes space control as:

> Space Control…[offensive space control] (OSC) measures taken to prevent an adversary's hostile use of US/third-party space capabilities or offensive operations to negate an opponent's space capabilities used to interfere with or attack US/allied space systems.[52]

Like space operations, cyber operations require control of advantageous position in cyber-infrastructure and logical space.

Cyberpower resonates with the experience of Desert Storm commanders. Air Force General Benard predicted that precision guided munitions by space age fighters could defeat Warsaw Pact "follow-on forces" and thus support AirLand Doctrine.[53] Precision guided munitions provided the

---

[48] Walter J. Boyne, *The Influence of Air Power Upon History* (New York: K. S. Ginger Company, 2003), 139.

[49] Boyne, *Influence of Air Power Upon History,* 143-5.

[50] Klein, *Space Warfare*, 81-3.

[51] Ibid, 84.

[52] Joint Publication (JP) 3-14, *Space Operations* (Washington, DC: Government Printing Office, 2013), xi.

[53] Stephen Bundiansky, *Air Power: The Men, Machines, and Ideas That Revolutionized War, From*

Central Command (CENTCOM) Commander, General Schwarzkopf, the ability to cut off supplies, isolate the Iraqi regime from ground forces, and disable air-defense assets.[54] Potentially, cyber forces can be employed to achieve similar functions through the use of its unique attributes. Either space or cyber domains enable precision guided munitions essential for a minimalist operational approach.

Echevarria describes the tension within operational art regarding the balance between cross-domain forms of warfare and local tactical capabilities:

> "[O]perational art is nothing without operational capability. The lack of operational-level experience was a significant shortcoming that plagued US Forces for the first few years of [World War II]…Forward movement of ground forces often employed the need to capture another airfield so that air cover could extend the depth of a theater; thus, fire and movement, always mutually reinforcing on a tactical level, had been mutually dependent on an operational one."[55]

Cyberspace is more than a topography of land maneuver. Antoine Bousquet questions the conclusions of Cebrwoski and the NCW concept as opposed to Boyd's cybernetic theory; observe, orient, decide, and act (OODA) loop. Bousquet concludes that Boyd sought to get inside an opponent's OODA cycle as an approach to achieve initiative, surprise, and deception beyond simply speed.[56] Thus connecting Leonhard's concept of perception and tempo to Bousquet's critique of net-centric warfare enables a framework to see cyber warfare on the battlefield as an indirect means to overwhelm an opponent's offsets within a respective domain.[57] Cyberspace developed after Desert

---

Kitty Hawk to Iraq (New York: Penguin Books, 2005), 410.

[54] General Accounting Office (GAO), "GAO/NSIAD-97-134 Operation Desert Storm Air Campaign," *Report to the Ranking Minority Member, Committee on Commerce, House of Representatives* (Washington, DC: US General Accounting Office, June 1997), 67-77; Bundiansky, *Air Power*, 422.

[55] Echevarria, "American Operational Art, 1917-2009", 148.

[56] Bousquet, *The Scientific Way of Warfare*, 195.

[57] Leonhard, *Fighting by Minutes*, 17-18.

Storm to generate new tempos and topographies that remained fertile to manipulation; the cyber domain is corruptible and transmutable.

This paper relies on five characteristics of cyberspace as the basis of analysis for the further study. First, cyberspace requires man-made physical nodes within its topography. Second, control of advantageous positions in the cyber infrastructure and logical space enables warfare. Third, cyberpower cannot succeed by opposing cyber forces but through the manipulation of cyber topography. Fourth, cyber dominance enables the operational reach of cyber power through advantageous position and tempo. Fifth, defense of safe cyber-ports ensure the stability of cyber topography and the lines of communication to other domains.

Cyberspace is a complex adaptive system, second only to the natural world, in which manipulations of the system cause chaotic cascading effects. Achieving a position of advantage in cyberspace can theoretically be attained through maneuver in other domains. William Lind rhetorically asks, "Why is operational art important if you are to do maneuver warfare? Because it is through excellence in the operational art more than through manoeuver in the tactical battle that a smaller force can defeat a larger one."[58] Robert R. Leonhard contemplates that the natural domains of warfare remain confined within time to choose between measures of movement, striking, and protection; cyberpower can do all these simultaneously. The operational artist arranges resources in time to actions in advantageous sequence and synchronous events.[59] Offensive cyber activities rely on the enemy's infrastructure. The act of the sequencing of actions in time creates a frequency that cyberspace can amplify through harmonization.

Cyber power can provide depth, speed, and duration of physical, tactical events that contribute to operational tempo and circumvent an opponent's ability to react.[60] John Boyd posited

---

[58] Williams S. Lind, *Maneuver Warfare Handbook* (Boulder: West View Press, 1985), 23-4.

[59] Leonhard, *Fighting by Minutes*, 17-20.

[60] Ibid, 70-72.

that the relationship of the Second Law of Thermodynamics interacts with the cognitive reality. Entropy acts and multiplies penetrations into an opponent's decision cycle resulting in cognitive paralysis.[61] Frans Osinga summarized Boyd's ideas as military formations and their political employers' metaphorically behave as organic systems: both complex adaptive systems and open systems that decay as used.[62] Cyberspace catalyzes the enemy's world like the final drive of an engine made to propel their "organic" system of control and cognitive reality in a negative direction.[63]

During the research, no other theory of operational art connected cyberspace to joint operations. However, three topics appeared that have contributed to the development of theory to provide for a structured focused case study. Matthew Miller, Jon Brickley, and Gregory Conti explored the misperceptions and difficulty of applying physical principles of warfare to cyber operations.[64] Talon G. Anderson addressed cyber operations as a means of asymmetric warfare within the information environment.[65] Tom Gjelten's article "First Strike: US Cyber Warriors Seize the Offensive" provided an example of the volumes of articles, op-eds, and dissertations that weave the latest events of cyber power with military strategy.[66]

---

[61] John R. Boyd, "Destruction and Creation," Unpublished Paper (September 3, 1976): 1, retrieved from http://dnipogo.org/john-r-boyd/; Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (New York: Routledge, 2007), 80. Osinga summarizes Boyd's Observe, Orient, Decide, Access (OODA) loop as a cybernetic system in which each node affects the state of the next.

[62] Osinga, *Science, Strategy and War*, 124.

[63] Robert Axelrod and Michael D. Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier* (New York: Basic Books, 2000), 30. Cyberspace acts like a variable causing a closed system to open and transform rapidly in response.

[64] Matthew Miller, Jon Brickey, and Gregory Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong," *Small Wars Journal* (November 29, 2012), accessed October 3, 2016, http://www.smallwarsjournal.com/printpdf/13573.

[65] Talon Anderson, "Adapting Unconventional Warfare Doctrine to Cyberspace Operations: An Examination of Hacktivist Based Insurgencies," Monograph (Fort Leavenworth: US Army Command and General Staff College, 2015).

[66] Tom Gjelten, "FIRST STRIKE: US Cyber Warriors Seize the Offensive," *World Affairs* 175, no. 5 (January/February 2013): 33-43; Thomas Rid and John Arquilla, "Think Again: Cyberwar," *Foreign Policy*,

Cyber-land operations theory requires a starting point. Bradley Converse and Scott Applegate's research provided a basis to support research for cyber-land interactions. Converse and Applegate employed the frameworks of air power and the principles of war respectively to develop the joint conceptual possibilities of cyber operations.[67] From each of these papers, the study built a structure of relationships for a methodology and structure to grow upon the dominant operational cyber theory. However, a gap remains in the study of cyber and operational art. The study applies cyber power as a theoretical warfare framework that combines the utility of cyberspace and operational art in warfare.

Methodology

This study utilizes the structured focused approach of a single case study to construct findings that indicate the interaction that cyber operations enhance cross-domain warfare. The Russo-Ukrainian conflict provided evidence to support the research questions using the device of cyberspace characteristics. The five characteristics of cyberspace regarding the research questions frame the effectiveness of operational art in the scope of cross-domain warfare. The structured focused methodology provided a way to assess the evidence that cross-domain warfare occurred in the Ukrainian theater.

How land and cyber operations mutually impacted strategic outcomes regarding the operational reach and tempo suggests a complex interaction between land and cyber operations. The research suggests that actors can exploit the concepts of chaos theory, systems theory, and

---

no. 192 (March/April 2012): 80-4; Lloyd Wihl, Maneesh Varshney, and Jiejun Kong. "Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments," *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) Paper, no. 10313,* (Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), 2010).

[67] Bradley D. Converse, "Cyber Power and Operational Art: A Comparative analysis with air power," Thesis (Newport, RI: Naval War College, 2013), 1; Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *4th International Conference on Cyber Conflict* (2012): 183

organic systems to achieve temporal dominance. Cyber power appears to alter the time, space and purpose of land power regarding operational reach and tempo. The two case study questions filtered the characteristics of cyber and provided a basis to assess the critical events for a cyber-land harmonic interaction.[68]

This monograph uses two standardized research questions founded with the characteristics of cyberwarfare. First, how the Russian Federation applied joint operations with cyberpower and exploited the characteristics of cyberspace to enable operational reach and tempo. The observed interactions between land and cyber in the case study provide evidence that land and cyber maneuvers achieve operational synergy and a potential harmony. If the Russian Federation appreciated the interaction of land and cyber, then they would operationalize and synchronize each within a symbiotic-strategic setting. Secondary sources supported observations that the Russian Federation cyber-actions to provide evidence that cyber and land force synchronization transformed mutual operational reach. Observed synchronous land and cyber applications construct a picture of operational tempo that transfigured the time, space, and purpose of events toward strategic aims.

The case study filtered events using validated observations in both domains of warfare. The assessments identified and supported predictions that land and cyber maneuvers enhanced cross-domain actions. Non-governmental sources, the open press, and the North Atlantic Treaty Organization (NATO) publications provided the bulk of information about the conflict. The study assumed that the Russian Federation manipulated the eastern European press. The study discounted many of the Russian media sources as manipulated observations based off of the construct of the Russian application of "reflexive control." Additionally, evidence from the Ukrainian ministry investigations provided a counter-perspective to Russian sources. Ultimately, global non-governmental post cyber-forensic evaluations tied the actions of Russian land and cyber forces to

---

[68] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: MIT Press, 2005), 69.

clarify a picture of events. The critical events between cyber and land domains indicated a new impact of cross-domain activities.

The structured focused approach methodology applied to the Russo-Ukrainian conflict facilitated the objectives of this monograph. Above all, the balance of sources against possible cyber and attributional events determined the scope and tempo of operations in the Ukraine. The justified hypothesizes suggest that cyber warfare exposed a new approach in operational art through synchronous cross-domain implications.

Cross-Domain Changes to Cyberspace

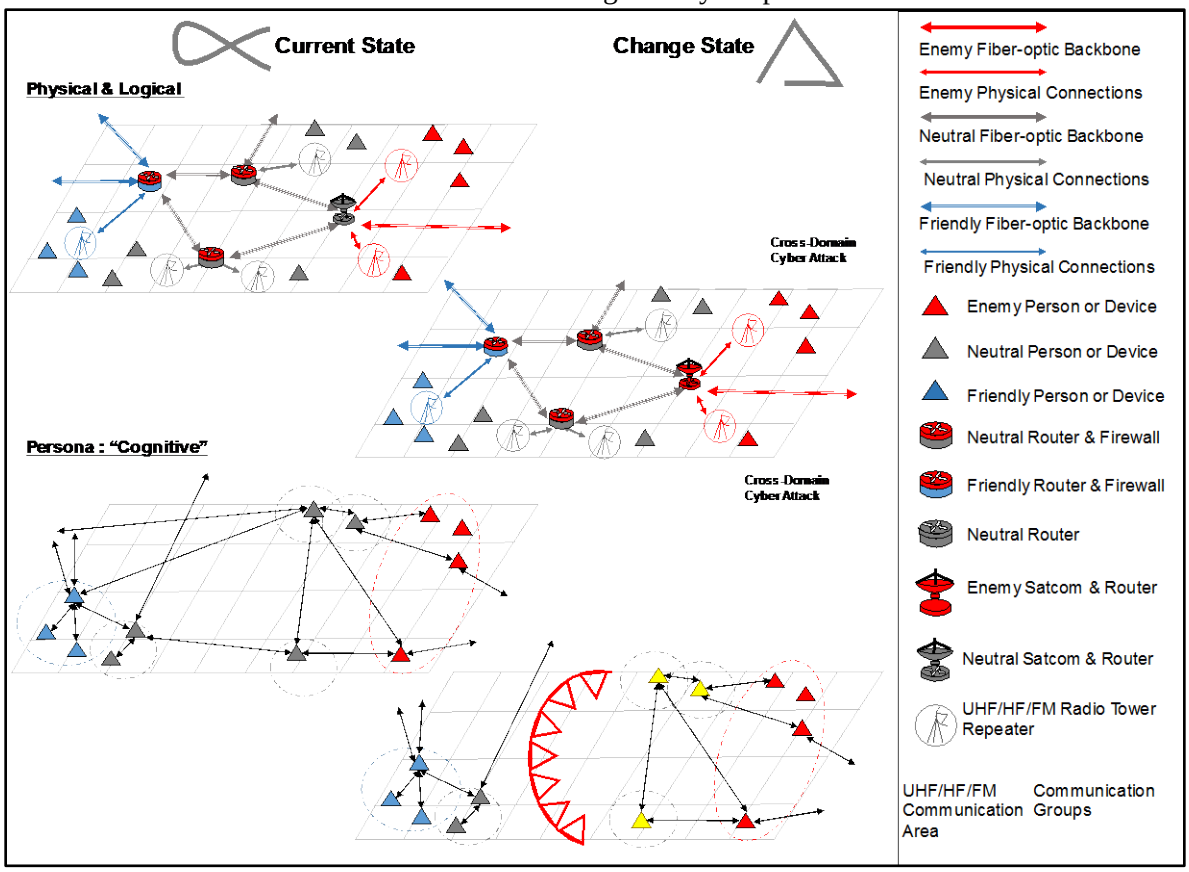

Figure 3.1. Layers of Cyberspace Manipulation. Blue forces redirected in cyberspace after Red Force destroys or manipulates the physical/logical nodes. Blue force cognitively separated from isolated elements.

Case Study: The Russo-Ukrainian Conflict 2013 to 2015

The combined operations between the Russian land and cyber forces leveraged several advantages against the Ukraine between 2013 and 2015. Ukrainian cyber architecture and topological environment created a familiar set of considerations that Russian troops continually addressed through modification of their operations. The Russian land forces synchronized cyber and ground troops that diverged from the classical operational art of “deep battle” within the context of cross-domain warfare. The Russian Federation maneuvered on land to affect cyber and vice versus. The case study provides evidence of the mutual impact of land and cyber power. The case study presents evidence that the characteristics of cyberspace alter the application of operational art regarding cross-domain warfare.

Modern Russian Theory of Warfare

Multiple American analysts assess "reflexive control" as the employment of all twenty-first-century capabilities of national power into the frameworks of "deep battle" operations that manipulate an enemy. V.A. Lefebve first introduced the concept of reflexive control in the 1960s. “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.” According to Bret Perry in Small Wars journal, *Maskirovka: deception* is a fundamental element in the theory reflexive control.[69] USSR special reconnaissance missions supported Soviet deep battle operations with shaping efforts that would create the space of future decisions [70] The Russian Federation

[69] Brett Perry, “Non-liner Warfare in Ukraine: The Critical Role of Information Operations and Special Operations,” *Small Wars Journal*, August 14, 2015, accessed August 30, 2016, http://smallwarsjournal.com/printpdf/27014.

[70] “Reconnaissance carried out to subvert the political, economic, and military potential and morale of a probable or actual enemy. The primary missions of special reconnaissance are acquiring intelligence on major economic and military installations and either destroying them or putting them out of action; carrying out punitive operations against rebels, conducting propaganda; forming and training insurgent detachments,

employed cyberpower as another part of the framework of reflexive control equal to other military domains to create the positive environment for military action.

The Russian's employ conventional forces as a phase of escalation to finalize an opponent nation into accepting the desired state. Russian Chief of the General Staff Valery Gerasimov says that the open use of force comes from a stage following the manipulations of information and actions used by special forces. Above all Gerasimov declared that extensive use of force should be employed as the final step to conflict success.[71] Maria Snegovaya, an expert in Russian political science from Columbia and the Wilson Center, states that reflexive control is not only the Kremlin's information warfare but an innovation of thought from Soviet doctrine.[72] The Ukrainian experience of reflexive control should not be seen as something new but an adaption of deep battle.

Snegovaya captures three key elements of Russia's reflexive control techniques. First, denial and deception operations concealed or obfuscated the presence of the Russian forces in Ukraine. Second, the Russian Federation disguised goals and objectives that generated an acceptable conclusion within the Kremlin's aims. Third, the Russian Federation justified its action through superficially plausible international legality. NATO assessed that the Russians exploited

---

etc. Special reconnaissance...is conducted by the forces of covert intelligence and special purpose troops." Fleet Marine Force Reference Publication (FMFRP) 3-201, *Spetsnaz* (Washington DC: Department of the Navy, January 18, 1991), accessed March 10, 2015, http://cnqzu.com/library/Anarchy%20Folder/Military%20Reference%20and%20History/Spetsnaz%20-%20FMFRM%203-201.pdf.

[71] "All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces – often under the guise of peacekeeping and crisis regulation – is resorted to only at a certain stage, primarily for the achievement of final success in the conflict." Valery Gerasimov, "The Value of Science in Prediction: New Challenges Require Rethinking on the Forms and Methods of Warfare," *Military Review* (January-February 2016): 23-9, last accessed August 30, 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

[72] "All of the underlying concepts and most of the techniques were developed by the Soviet Union decades ago. Russian strategic theory today remains relatively unimaginative and highly dependent on the body of Soviet work with which Russia's leaders are familiar. Russian information operations in Ukraine do not herald a new era of theoretical or doctrinal advances, although they aim, in part, to create precisely this impression." Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," *Russia Report I* (Washington, DC: Institute for the Study of War, September 2015): 7.

cyber campaigns in Georgia and the Ukraine with applied "continuous, mounting pressure on the Georgian [and Ukrainian] government and population… to provoke the Government[s] into the desired decisions and actions,"[73] that satisfied the strategy of reflexive control. The three reflexive control elements combined to limit NATO military power along with the threat of the Russian military nuclear potential.[74]

The infrastructure of the opponent remains key to the employment of cyber and information capabilities by the Russian Federation. Bedritsky pointed out that rather than improving the efficiency of traditional military operations, the new information [cyber/technosphere] warfare campaigns would attempt to destroy pieces of the enemy's critical infrastructure. Hence, cyber-means such as cyber-attacks can cause a failure of power supply facilities, transportation infrastructure, government institutions, etc. In this way, cyber warfare can induce the target country's political and economic collapse.[75]

Bedritsky's "Information Warfare" should not be confused as it is in the context of pre-2014 American definition with cyberwarfare (Information Warfare). Russia's new military doctrine for propaganda and information war theories have not changed from the old Soviet Union.[76] However, Yu. I. Starodubtsev, V. V. Bukharin, and S. S. Semyonov coined the Russian term for cyberwarfare as "Technosphere Warfare." These authors stated that "it is not always economical to employ an armed force that can only be committed when a conflict reaches an extreme." Strategic

[73] North Atlantic Treaty Organization, "Analysis of Russia's Information Campaign Against Ukraine: Examining Non-Military Aspects of the Crisis in Ukraine from a Strategic Communications Perspective," Report (Riga, Latvia: NATO StratCom Centre of Excellence, December 1, 2016): 35.

[74] Snegovaya, "Putin's Information Warfare in Ukraine," 7.

[75] Ibid, 14.

[76] "Doctrinal assumptions about information warfare demonstrate not so much a change in the theory of its conduct... but rather a clinging to old methods (sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population)." Jolanta Darczewska, "The Devil Is In The Details: Information Warfare In The Light Of Russia's Military Doctrine," *OSW Point of View*, no. 50 (May 2015): 7.

goals within the construct of reflexive control can be better achieved through computer network attack on automated control systems (ACS). The technosphere theory, "a concept of an entirely new type of warfare—warfare in an artificial environment" mirrors the western concept of cyber warfare.[77]

The structure and maturity of Ukrainian cyberinfrastructure provide a relevant sample of cyber-land warfare. Ukraine entered the Information Era immediately after the dissolution of the Soviet Union in 1991. Keith Giles from the Conflict Studies Research Centre noted that the Russian Federation developed and financed the Ukraine's communication systems and telecommunication companies. Additionally, the Ukraine uniquely bore a single physical fiber-optic line to mainland Crimea in 2013.[78] The remainder of Ukrainian information architecture tied to the main cities parallel with the intersections of railroads throughout the country. The symmetry between Ukrainian rail and cyberinfrastructure resonated with the conceptual patterns of deep battle and reflexive control theories.

The characteristics of cyberspace with operational art escalated political events. NATO tensions began to grow as early as March 29, 2008 when the Russians began to express opposition to NATO membership for Georgia and the Ukraine.[79] Underlying the Russian fears of NATO

---

[77] "A form of conflict in which the targets attacked (protected) and attack (protection) capabilities are information existing within the single worldwide telecommunications environment (SWTCE). In this context, information is more than data transmitted through (stored in) SWTCE: it is also information about the status of SWTCE (or its parts) and that of the ACS of the system attacked and their operating algorithms." Yu. I. Starodubtsev, V. V. Bukharin, and S. S. Semyonov, "Technosphere Warfare," *Military Thought: Voennaya Mysl'*, no. 7 (2012): 22-31.

[78] "Ukraine's more interconnected nature makes it impossible to restrict access to the internet overall, except in the very special case of the Crimean Peninsula. But also, there is no reason why Russia should try, especially given the integrated nature of Ukrainian and Russian information space. Since Russia already enjoyed domination of Ukrainian cyberspace, including telecommunications companies, infrastructure, and overlapping networks, there was little incentive to disrupt it. In short, Russia had no need to attack that which it already owned." Keir Giles, "Russia and Its Neighbours: Old Attitudes, New Capabilities," *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015): 24.

[79] Thomas, *Russia Military Strategy*, 372.

expansion, the threat to Russian Federation interests included influence over oil from Azerbaijan and the Middle East through the Turkish pipeline and domestic Russian controlled pipelines that run around the Black Sea region to European markets.[80] Further, the Russian Federation gained military strategic control of the warm water port at Sevastopol. Thus, Ukraine dominated Russian calculus.[81] Finally, the historical regional hegemony of the Russian people since the Crimean War, World War II, and the Soviet Union generated a condition of honor for President Putin's thinking materialized in the form of the Collective Security Treaty Organization.[82] NATO expansion and Ukrainian departure from the Russian sphere of influence threatened petrol-economic interests, fear of NATO military expansion, and honor of Russian hegemonic memories.

The cyber operations coincided with the Russian strategic objectives expressed on February 13, 2008 after Ukrainian President Victor Yushchenko attempted to soothe the Russian concerns over Ukrainian entrance to NATO.[83] The Russian approach included the employment of cyber reconnaissance as early as 2009 to support the Russian Federation strategic considerations. Cyber security firm iSight traced the earliest Russian Military Intelligence Directorate (GRU) cyber operations in the Ukraine and NATO to the Sandworm Operation in 2009.[84] Underlying all the

---

[80] Alexander J. Motyl, "The Sources of Russian Conduct," *Foreign Affairs* (November 16, 2014), accessed August 30, 2016, https://www.foreignaffairs.com/articles/russian-federation/2014-11-16/sources-russian-conduct.

[81] "'The prolongation of the Black Sea Fleet's presence in Sevastopol is essential to Russia,' Yanukovych said on Wednesday. 'We understand that the Black Sea Fleet will be one of the guarantors of security on the Black Sea.'" Ivan Watson and Maxim Tkachenko, "Russia, Ukraine agree on naval-base-for-gas deal," *CNN.com*, modified April 21, 2010, accessed October 15, 2016, http://www.cnn.com/2010/WORLD/europe/04/21/russia.ukraine/index.html?hpt=T2#.

[82] Leon Aron, "The Putin Doctrine: Russia's Quest to Rebuild the Soviet State," *Foreign Affairs*, (March 8, 2013), accessed October 16, 2016, https://www.foreignaffairs.com/articles/russian-federation/2013-03-08/putin-doctrine.

[83] Peter Finn, "Putin Threatens Ukraine On NATO," *The Washington Post*, modified February 13, 2008, accessed October 16, 2016, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/12/AR2008021201658.html.

[84] iSight Partners, "Russian Cyber Espionage Campaign – Sandworm Team," *iSight Partners Report* (2014): 1-11, quoted by Unwala and Ghori, "Brandishing the Cybered Bear," 4. The Sandworm espionage operation, which exploited a previously unknown Windows vulnerability, had started as early as 2009 and

tensions remained the risk to the Russian petrol-energy economics including Gazprom and the debt of approximately $1.5 billion.[85]

The Russians could not secure their interests with the ouster of Victor Yushchenko by Victor Yanukovych. While Yanukovych immediately withdrew NATO application, he also aligned with outside petrol-interests.[86] Yanukovych under domestic pressure signed a 50-year production sharing agreement on January 24, 2013 with Shell Oil to exploit the Yukivska shale oil field as the first step for Ukrainian independence from Russian gas.[87] The Russian leadership quickly expanded cyber espionage with Operation Sandworm and began to set in place "Operation Armageddon" which emplaced cyber warfare access points for future operations. According to LookingGlass cyber threat firm, "Operation Armageddon" initially provided military advantages over the target Ukrainian government, law enforcement, and military officials which would provide near-term Ukrainian policy and emerging military strategies.[88]

Events in the Summer of 2013 generated further concern for the Russian interests as the Ukraine began to finalize discussions to accept the Association Agreements with the European Union. On June 26, 2013, Russian cyber forces began manipulation of Ukrainian information

---

targeted EU and NATO telecommunications infrastructure through 2014. Sandworm's malware had intensified and focused Ukrainian government networks during September 2014, which coincided with the NATO summit in Wales.

[85] Rosalind Ryan, "Join NATO and we'll target missiles at Kiev, Putin warns Ukraine," *Reuters*, modified February 12, 2008, accessed October 15, 2016, https://www.theguardian.com/world/2008/feb/12/russia.ukraine; Thomas, *Russia Military Strategy*, 372.

[86] Adam Taylor, "That time Ukraine tried to join NATO – and NATO said no," *The Washington Post*, modified September 4, 2014, accessed October 15, 2016, https://www.washingtonpost.com/news/worldviews/wp/2014/09/04/that-time-ukraine-tried-to-join-nato-and-nato-said-no/.

[87] Richard Balmforth and Dmitry Zhdannikov, "UPDATE 1-Ukraine signs landmark $10 bln shale gas deal with Shell," *Reuters*, modified January 24, 2013, accessed October 15, 2016, http://www.reuters.com/article/shale-ukraine-idUSL6N0ATER320130124.

[88] Jason Lewis, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," *LookingGlass Cyber Threat Intelligence Group* (Baltimore, MD: LookingGlass Cyber Solutions, April 28, 2015), 3.

systems.[89] A month later the Russian cyber forces emplaced remote manipulator systems (RMS) and remote access tools (RATs).[90] Russian intentions and concerns became more intense by September 2, 2013, when cyber-attacks on all parties began days before the 10th Yalta Annual Meeting for Ukrainian entrance into the European Union system. Cyber threat experts believe these attacks sought to determine the political decisions by all parties.[91]

The critical political point that drove the Russian Federation decision to seize the Crimea and then extend to eastern Ukraine occurred around November 2013 that became known as Euromaidan. Ukrainian President Victor Yanukovych suddenly pulled out of European Association Agreements sparking widespread protests and riots throughout western Ukraine. Domestic unrest by the ethnic-Ukrainian population countered the Russian interests and threatened local investments.[92] Russian Federal Security Service (FSB) with the integration of still friendly Secret Service of Ukraine systematically shut down mobile operators with armed police suppression. Finally, on December 2, 2013 opposition websites fell to Distributed Denial of Service (DDoS) attacks from commercial botnets employing cyber weapons attributed to the Russian Federation. On

[89] Jason Lewis, "Operation Armageddon," 18. The earliest known file modification timestamp by Russian cyber attack of a file used ("den.exe") is identified.

[90] "August 27-30, 2013, The first known variant of RMS RAT (MD5: 2DD8A3312635936041C686B5FC51C9FF, described is identified along with "den.exe" (MD5: 40F7CC7F30C30C79AD7541A4CF0BF72B). The "den.exe" malware is used to modify an infected system's DNS servers to the following, to perform DNS redirection (or hijacking) attacks using the first IP address as a malicious DNS server along with a legitimate OpenDNS server… The inclusion of the legitimate OpenDNS to DNS provider suggests that the malware only uses the attacker-controlled DNS server to resolve specific domains of interest to the attackers…[T]he domain file-attachments.ru was privately registered via the REGRU-RU registrar for use in future attacks. The first known IP resolution was 46.254.20.155." Jason Lewis, "Operation Armageddon," 18.

[91] "The goal of these attacks is to gain insight into the political decisions being made at this time. Attackers utilized the RMS RAT as well as "den.exe."" Jason Lewis, "Operation Armageddon," 19; Tony Martin-Vegue, "Are we witnessing a cyberwar between Russia and Ukraine? Don't blink – you might miss it," *Cyber Security Online*, modified April 24, 2016, accessed August17, 2016, http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html.

[92] British Broadcasting Company, "Ukraine PM Mykola Azarov warns of coup in the making," *BBC*, modified December 2, 2013, accessed October 15, 2016, http://www.bbc.com/news/world-europe-25192792.

February 21, 2014 Ukrainian President Yanukovych escaped to the Russian Federation signaling the trigger for the Russian forces seizure of Crimea.[93] Perceived Russian interests of regional hegemony, petrol-economy, and the naval base in Ukraine could no longer be secured through subtle and informational manipulation alone.

Land Operations Enhance Cyber Operational Reach

The Russian Federation use of operational art mutually employed both land and cyber operational reach within the Ukraine around February 2013 within the lens of "reflexive control." The Russian cyber operations sought to isolate the information flow of the Ukrainian government from institutions and military forces across the Ukraine. The Russian land forces altered the physical infrastructure within Crimea, enabling cyber operations through canalizing Ukrainian cyberspace. Similarly, cyber-land operations employed the same tactics as the conflict spread to eastern Ukraine. Cyber operations expanded to enable precision fires and defined operational timelines for land forces. The correlation of terrestrial and cyber maneuvers suggest that land and cyber operations mutually enhanced operational reach.

On February 27, 2014, *Spetsnaz* forces were put on alert and mobilized. The task organized Special Operations Command (KSO) and the 45th opSpN (Independent Special Purpose Regiment of *Spetsnaz* detached to the 45th Russian Airborne Troops (VDV)) disembarked by air transport at the naval base in Sevastopol. KSO forces seized the Crimean parliament building, the Simferopol airport, and key Ukrainian military facilities. Similar unmarked soldiers took over a Ukrtelecom building in Sevastopol. Ukrtelecom, Ukraine's National Telecommunications operator, subsequently issued a report claiming that the soldiers "seized several communications hubs in Crimea," tampered with Crimean fiber-optic cables, and damaged its optical fiber and conductor

[93] British Broadcasting Company, "Putin: Russia helped Yanukovych to flee Ukraine," *BBC,* modified October 24, 2014, accessed October 16, 2016, http://www.bbc.com/news/world-europe-29761799; Bret Perry, "Non-Linear Warfare in Ukraine," *Small Wars Journal.*

units. (Figure 4.1 depicts the Russian operation in Crimea). Soldiers also manipulated the remaining active fiber optic cables with data intercept devices.[94] Effectively, the land forces used physical control of to generate cyber power throughout the Crimea.

No reported sophisticated cyber exploits were required to isolate cyberinfrastructure as KSO forces seized the Simferopol Internet Exchange Point (IXP) and selectively disrupted cable connections to the mainland."[95] Infantry from the 810th Marine Infantry Brigade on March 1st and March 17th seized airports, surface-to-air missile batteries, Ukrainian military bases, military hospitals, and fuel depots.[96] The Russian land forces completed the isolation of the Crimean peninsula from Ukrainian cyber forces.

Subsequently, the Russian cyber forces enabled the KSO control of Ukrainian telecommunications facility.[97] The logic behind these comes from the Ukraine's telecommunications geography. Ukraine's Internet Service Providers (ISPs) were decentralized and held terrestrial and satellite path diversity to the rest of the world. Crimea was one of the vulnerable areas in Ukraine since it only held one Internet Exchange Point (IXP) that connected the peninsula to the rest of the country. If Crimea's IXP were damaged or shut down, Crimea would be

---

[94] "Feb. 28 Updates on the Crisis in Ukraine," *The New York Times*, modified February 28, 2014, accessed October 1, 2016, http://thelede.blogs.nytimes.com/2014/02/28/latest-updates-tensions-in-ukraine/.

[95] "When Russia wished to isolate Crimea from news from the outside world, no sophisticated cyber exploits were required. Instead, SOF detachments simply took over the Simferopol IXP and selectively disrupted cable connections to the mainland." Giles, "Russia and Its Neighbours: Old Attitudes, New Capabilities," 25.

[96] "March 1 and March 17th, these forces allegedly conducted 16 different seizure operations—9 of which were confirmed to be immediately successful. Targets ranged from airports, surface-to-air missile batteries, Ukrainian military bases, military hospitals, and fuel depots." Perry, "Non-Linear Warfare in Ukraine," *Small Wars Journal.*

[97] Martin-Vegue, "Are we witnessing a cyber war…?" *Cyber Security Online*; Ukretelcom, "Ukrtelecom's Crimean sub-branches officially report that unknown people have seized several telecommunications nodes in the Crimea," last modified February 28, 2014, last accessed October 1, 2016, http://en.ukrtelecom.ua/about/news?id=120467; NATO "Analysis of Russia's Information Campaign Against Ukraine," 29.

completely isolated, allowing Russia to control the region's communications.[98] Also, actions by coordinated pro-Russian hackers disrupted the mobile phones of members of the Ukrainian parliament.[99] Continuous cyber attacks on mainland Ukraine maintained external isolation of Crimea hours before the invasion.

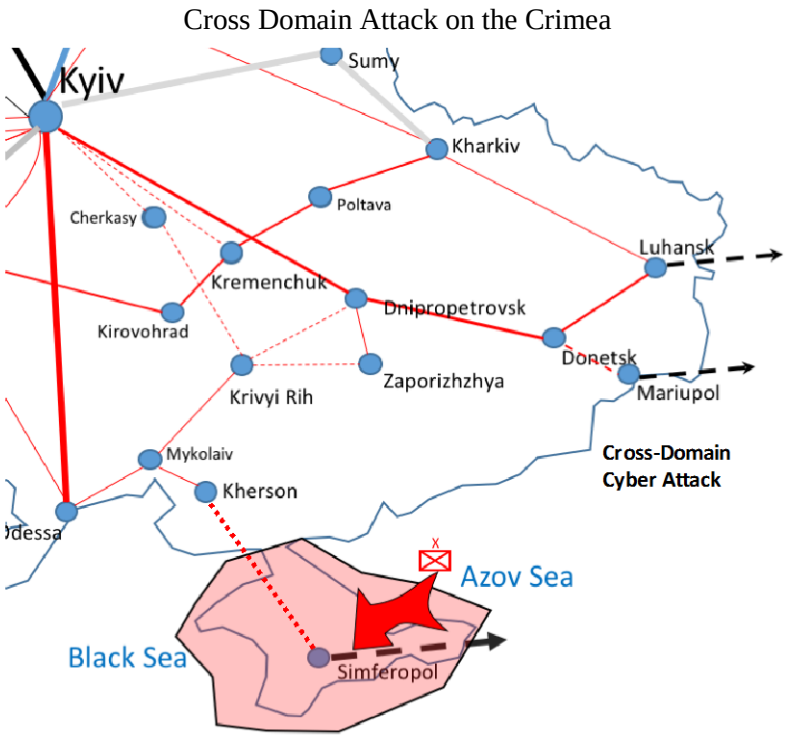

Figure 4.1. Crimean land and cyber-attack: cross-domain attack. The attack on Crimea to seize ISP/IXP (internet exchange points and alter the physical cyberspace.) Fiber optic line image adapted from: European Research Council, "Ukraine Fiber Optic Line," modified 2015, accessed October 21, 2016, http://infrastructure.kiev.ua/upload/Fiber.png.

[98] Sanja Kelly et al., "Freedom on the Net 2014," *Freedom on the Net* (Freedom House, 2014): 820-1; Jason Rivera, "Has Russia Begun Offensive Cyberspace Operations in Crimea?" *Georgetown Security Studies Review* (March 2, 2014), http://georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea/.

[99] Martin-Vegue, "Are we witnessing a cyber war…?" *Cyber Security Online*; Reuters, "Ukraine says communications hit, MPs phones blocked," *Reuters*, March 4, 2014, http://www.reuters.com/article/2014/03/04/ ukraine-crisis-cybersecurity-idUSL6N0M12CF20140304.

On March 2, 2014, the Russian infantry reinforced the KSO in Crimea with little resistance. The combined attacks on Ukrainian and Crimean telecommunications before Russia's invasion and post-invasion cyber-attacks significantly lowered the response potential of the Ukrainian government.[100] Operations Armageddon and Sandworm altered the cognitive space through integrated cyber and land force maneuvers.

"Reflexive Control" doctrine along with "deep battle" again began to materialize in eastern Ukraine supporting the hegemonic strategic objectives of the Russian Federation. Isserson's composite theory of "multi-level battle waged on several tiers within the operational depths" took a new form in the Donbass Campaign.[101] The threat of the Russian invasion further escalated by March 12, 2014 as NATO and the Ukrainian government identified the Russian Federation forces massing along Ukraine's eastern border.[102] On April 27, 2014 *The Sunday Times* reported that 300 elite special operatives which include commandos with combat experience in Chechnya and Georgia had infiltrated Ukraine to spread pro-Kremlin sentiment among local Russian speakers. "They are recruiting paramilitary fighters in exchange for cash handouts and waging a sophisticated propaganda war," said Colonel Vialy Naida, the head of Ukrainian counterintelligence.[103] Between April 15, 2014 and April 30, 2014, cyber infiltration shifted from gathering political strategies to

[100] Unwala and Ghori, "Brandishing the Cybered Bear," 6-7.

[101] Isserson, *The Evolution of Operational Art*, 67-8.

[102] Tzvi Kahn and Evan Beese, "FPI Fact Sheet: Timeline of Russian Aggression in Ukraine and the Western Response," Report (Washington, DC: The Foreign Policy Initiative, September 18, 2014), 2; Steven Lee Myers and Alison Smale, "Russian Troops Mass at Border With Ukraine," *The New York Times*, last modified March 13, 2014, last accessed October 1, 2016, http://www.nytimes.com/2014/03/14/world/europe/ukraine.html?_r=1.

[103] Slovyansk Bojan Pancevski, "Putin's 300 whip up Ukrainian turmoil," *The Sunday Times*, last modified April 27, 2014, last accessed October 1, 2016, http://www.thesundaytimes.co.uk/sto/news/world_news/Ukraine/article1404493.ece.

military intelligence.[104] Again, the Russian forces began the process of integrating an operational approach between cyber and land forces.

Cyber capabilities escalated by June 15 as the Russian forces deceived Ukrainian defenses and prepared the next Russo-Ukrainian campaign. The cyber operation began and used the same malware and TTPs from the Crimea. LookingGlass hypothesizes that the Russian cyber forces reused old TTPs to determine how Ukrainian forces would respond. Less than a week later on June 20, Ukraine's new President Poroshenko announced a ceasefire two weeks before initiating a military ground operation against pro-Russian rebels in the Donbass *oblast*. Security firms and digitalattackmap.com confirm Russian military activity and cyber-attacks paused for those two weeks.[105] Presumably, the Russian GRU and FSB detected the intent to invade by Ukrainian forces through multiple intelligence sources including cyber reconnaissance and adapted a new operational approach.

New cyber TTPs and support by pro-Russian rebels amplified the land and cyber capabilities during the 2014 Donbass Campaign. Renewed, from July 17, 2014 – August 28, 2014, the Russian military invaded Ukrainian territory and large groups of Ukrainian forces became cornered and almost entirely destroyed. Shortly thereafter, the Ukrainian and Russian Presidents Poroshenko and Putin met. Poroshenko agreed to withdraw his forces. Only two days after their meeting on August 26, 2014, the cyber-attacks ceased.[106] The firsthand account by Glib Pakharenko

---

[104] "The first instance of a benign lure/decoy document [to military leadership] being used in a spear phishing email to convince victims to open malicious content is identified: "Списки без фотографий.docx," which translates from Russian to "Lists without photos.docx" (MD5: 7DF924CBB8A41B7622CDF4F216C63026). Operation Armageddon's name was derived from this document, which contains metadata showing it was both authored by and last saved by "Armageddon" (spelled incorrectly)." Lewis, "Operation Armageddon," 20.

[105] Lewis, "Operation Armageddon," 21; Arbor Networks, "Digital Attack Map," *Arbor Networks*, modified June 19, 2014, accessed October15, 2016, http://www.digitalattackmap.com/v1#anim=1&color=0&country=ALL&list=0&time=16240&view=map.

[106] Arbor Networks, "Digital Attack Map," August 25, 2014.

describes pro-Russian and *Spetsnaz* destroying physical cabling, broadcast infrastructure, and ATM networks. The destruction of communications architecture like in the Crimea isolated the Donbass.[107]

The seizure and alteration of the cyberinfrastructure along with a new employment of cyber TTPs extended the operational reach of precision artillery fires. Pakharenko in a NATO Cyber Center document observed that the Russian cyber capabilities culled data from GSM and Wi-Fi networks to adjust fire for artillery battalions.[108] Even while the expected ceasefire was to take effect, the Ukrainian forces came under artillery fires while Russia retained control of the *oblast* and massed artillery across the border.[109] The vast isolated cyber topography in the Donbass *Oblast* enabled almost omnipresent effects that extended from Donetsk to Luhansk.[110] Thus, even under the restricted strategic considerations of a ceasefire, Russia could maintain legitimate targeting in the eyes of enough of world powers to continue projecting the operational reach through cyber power.

The Crimean and Donbass campaigns of the Russo-Ukrainian conflict provide discreet examples of cross-domain maneuvers and the symbiotic beyond synergistic nature of operational reach in each domain. Crimea demonstrates the effect of land forces to alter cyberspace requirement

---

[107] Pakharenko, "Cyber Operations at Maidan: A First-Hand Account," 63; Arbor Networks, "Digital Attack Map," July 26, 2014.

[108] "Russian signals intelligence (SIGINT), including cyber espionage, has allowed for very efficient combat operations planning against the Ukrainian army. Artillery fire can be adjusted based on location data gleaned from mobile phones and Wi-Fi networks. GPS signals can also be used to jam aerial drones. Ukrainian mobile traffic can be rerouted through Russian GSM infrastructure via a GSM signaling level (SS7) attack; in one case, this was accomplished through malicious VLR/HLR updates that were not properly filtered." Pakharenko, "Cyber Operations at Maidan," 63.

[109] Ewen MacAskill and Shaun Walker, "Heavy shelling in Ukrainian port of Mariupol hours before agreed ceasefire," *The Guardian*, last modified September 5, 2014, last accessed October 3, 2014, https://www.theguardian.com/world/2014/sep/05/ukraine-heavy-shelling-hours-before-ceasefire-russia.

[110] "Fiercest fighting is near the town of Debaltseve, where the pro-Russian rebels are trying to surround Ukrainian troops. The town is a critical rail hub linking Donetsk and Luhansk." British Broadcasting Company, "Ukraine crisis in maps," *BBC*, last modified February 18, 2015, last accessed October 1, 2016, http://www.bbc.com/news/world-europe-27308526.

of man-made nodes that shape its topography. Also, the Crimean theater reveals that cyber power depends on the manipulation of topography to gain dominance. Donbass campaign demonstrates the ability of cyberpower to project control of infrastructure providing asymmetric effects. Asymmetric targeting such as cyber-enhanced physical ISR and adjusted virtual observation for accurate and timely fires. The Russian Federation operational art mutually suggests both land and cyber operational reach within the Ukraine.

Cyber Enhancement of Operational Tempo

Robert Leonhard proposed that the frequency of conflict impacts the consequence of employed tempo in warfare.[111] Conceptually, the impact of perceived and imperceptible tempos on the field of battle amplify the strategic employment of military force toward achievable ends. This study explores the Russo-Ukrainian conflict as pulses of events tied between cyber and land-cyber that achieved the outcomes by the Russian Federation. The Russians harmonized pulses in both cyber and land domains within their strategic framework of reflexive control. The initial tempo of tactical pulses occurred during the Euromaidan protests after the Russian's manipulated events and pressured political powers toward fulfilling their interests. The political unrest of Euromaidan allowed the Russians to prepare for the control of the Crimea and influence petrol-economic interests.

Leonhard describes tempo as the sequencing of event frequency and duration which provide opportunities for commanders.[112] The frequency of tactical events and aggregate pulses increased as the Russians transitioned to land invasion and overt cyberattacks. The operational tempo resulted in the strategic outcomes from the annexation of Crimea and semi-independence of

---

[111] Leonhard, *Fighting by Minutes*, 70.

[112] Leonhard, *Fighting by Minutes*, 11.

Donbass. The Russian intervention in Ukraine operationalized the construct of “Reflexive Control” to generate obstacles and circumstances that should have determined the logical course of Ukrainian and NATO politics. The events of the conflict indicate that the duration and frequency of cyber and land pulses are complimentary.

The Russian cyber events initially supported the sharp divergence of Ukrainian interests perceived by NATO and EU counter to Russian hegemonic sphere. The first pulse, the Russian Federation generated nationalism narrative under "Reflexive Control" to alter the discourse of international thinking. The second pulse, the Crimean excuse provided the Russian Federation with rapid means of control to gain the peninsula’s telecommunications infrastructure, severing cables and routing calls through Russian mobile operators. Ukrainian media companies lost their physical assets in Crimea, and local television programming shifted from Ukrainian to Russian networks.[113] The Russian Federation dominated local cyberspace to extend the effect of special forces involved in the operation, and points to an entirely new interface between cyber and information environments. The Russian cyber operations generated from physical seizure of fiber lines and imposed on Western planners the demonstrated cross-domain activities in eastern Ukraine.[114] The first round of conflict indicates that the Russian Federation gained advantages which overcame local circumstances and quickened both land and cyber operations.

The third pulse, cyber operations extended to cyber personas of commanders, Seizing opposition leaders identities, financial account takeovers, and espionage can be remarkably effective.[115] While the Ukrainian government and population balanced the Russian activities with NATO promises, the Russian Federation consolidated immediate gains. Forensic analysts like Tony

[113] Pakharenko, “Cyber Operations at Maidan,” 62.

[114] Keir Giles, “The Next Phase of Russian Information Warfare,” *Report* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, May 20, 2016): 13.

[115] Timothy L. Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth: Foreign Military Studies Office (FMSO), 2015), 399.

Martin-Vegue described the situation as, "[T]he opening days of a kinetic military operation, cyber-attacks [were] launched on telecommunications infrastructures. Russian multi-domain attacks avoided collateral damage within civilian infrastructure [with] the primary targets of government and military communications." Martin-Vegue also noted that distributed denial of service (DDoS) attacks provided the most cost effective attack to fix targets through cyberspace. The fourth pulse culminated on, February 27, 2014 with the Crimean Parliament seized by armed men. The Russian flag was raised over the region's capital.[116] By February 28, 2014, President Obama vowed, "The United States will stand with the international community in affirming that there will be costs for any military intervention in Ukraine."[117] The international political response and reaction came two weeks late. Time escaped the Ukraine and NATO which indicates that the frequency of had oscillated from an imperceptible to unacceptable levels.[118]

The Russian initial pulses in the Donbass indicate a suppression of decision to act by closing cognitive and temporal spaces. The Russians operated within the Ukraine and NATO OODA loops.[119] Political outcomes became tied between Ukrainian survival and American interests on March 2, 2014 with initial sanctions imposed on the Russian Federation.[120] The Russian GRU

---

[116] Kahn and Beese, "FPI Fact Sheet, 1; Reuters, "Timeline: Political crisis in Ukraine and Russia's Occupation of Crimea," *Reuters*, last modified March 8, 2014, accessed October 1, 2016, http://www.reuters.com/article/us-ukraine-crisis-timeline-idUSBREA270PO20140308.

[117] Kahn and Beese, "FPI Fact Sheet," 1; President Barack Obama, "Statement by the President on Ukraine," February 28, 2014, accessed October 2, 2016, https://www.whitehouse.gov/the-press-office/2014/02/28/statement-president-ukraine.

[118] Leonhard, *Fighting by Minutes*, 70. Leonhard describes four types of frequencies: imperceptible, unacceptable, difficult, typical. Leonhard's rates support the ideas of John Boyd and achieving cognitive dominance inside an opponent's OODA loop.

[119] Osinga, *Science, Strategy and War*, 80.

[120] "First, Ukrainian officials were unable to communicate with Crimean sources on the ground to acquire an accurate understanding of the ensuing conflict. Second, Ukrainian officials were unable to share information or execute command and control processes among themselves. Third, Ukrainian officials were unable to communicate with foreign allies, placate pro-Russian Ukrainians, or make efforts to undermine Moscow," Unwala and Ghori, "Brandishing the Cybered Bear," 6-7.

and FSB attacked to achieve changes in Donbass from March 2014. Pro-Russian's cyber attacked with prolonged DDoS attacks against Ukrainian and NATO media outlets.[121] Operational tempo still clearly favored the Russian strategic objectives because they still outpaced Ukrainian and International responses as they became perceived.

A sample bisection of the cyber pulse in May 2014 demonstrates the second cyber characteristic: control of advantageous positions in cyberinfrastructure and logical space enable warfare. Just 72 hours before the Ukrainian election the pro-Russian surge in Donbass occurred in May 2014. The pro-Russian insurgency opposed the mandate to the Ukrainian population for a legitimate pro-Western government. Alternately, the situation provided ethnic Russians with a clear choice to fight for Russian intervention. The election headquarters were hacked by the pro-Moscow group known as CyberBerkut. CyberBerkut attached government documents on its website and hacked the Ministry of Foreign Affairs and the Ministry of Defense. CyberBerkut, allegedly an independent Ukrainian organization, aligned rapidly and technologically with pro-Russian interests. Ukrainian officials suspect the Russian's enabled this group. Ukraine's two-decade old information systems predominately utilized Russian technology connected to servers located in Russia. The hacker tools employed against Ukraine were sophisticated, further indicating nation-state sponsorship.[122] The Russian objectives sought to control the Ukrainian governmental systems that would fall into the Russian Federation sphere of control. Temporal dominance by cyber pulses in Crimea appear to have invigorated the Russian Federation application of indirect cyber warfare.

---

[121] Martin-Vegue, "Are we witnessing a cyber war…?" *Cyber Security Online*.

[122] Margaret Coker and Paul Sonne, "Cyberwar's Hottest Front," *The Wall Street Journal*, 10 November 2015, A1 & A12; Petro Zamakis, "Cyber Wars: The Invisible Front," Ukraine Investigation, April 24, 2014, accessed October 15, 2016, http://ukraineinvestigation.com/cyber- wars-invisible-front/; Agence France-Presse, "Hackers Target Ukraine's Election Website," *Agence France-Presse*, October 25, 2014, accessed October 15, 2016, http://www.securityweek.com/hackers- target-Ukraine's-election-website.

The fifth pulse, the design of Russian systemic control in the Ukraine sought to re-dominate the Donbass region after the Ukraine began counterinsurgency operations. On April 18, 2014, during an interview, President Putin observed that parts of eastern and southern Ukraine were once part of "*Novorossiya*," and that "Russia lost these territories for various reasons, but the people remained." The czarist-era term refers to the period when the Russian Empire controlled much of Ukraine.[123] The temporal conflict extended rapidly past the Crimea to the Donbass within the narrative of the Russian Federation doctrine. Malware altered the Ukrainian electoral networks and achieved two divergent objectives. Hackers bolstered in-depth reconnaissance of their targets before any serious attack. Second, the hackers attacked to control technical credentials and prove the legitimacy of CyberBerkut. According to Nikolay Koval, if CyberBerkut really did exploit a new vulnerabilities, the group is likely supported by a nation-state (the Russian Federation).[124] The tempo of cyber operations exploited the construct of Ukrainian the strategic setting that enabled land operations in the Donbass to control cyberspace.

Cross Domain Attack in the Donbass

[123] Kahn and Evan, "FPI Fact Sheet, 2; Adam Taylor, "'Novorossiy,' the latest historical concept to worry about in Ukraine," *The Washington Post*, last modified April 18, 2014, last accessed October 3, 2016, https://www.washingtonpost.com/news/worldviews/wp/2014/04/18/understanding-novorossiya-the-latest-historical-concept-to-get-worried-about-in-ukraine/.

[124] Nikolay Koval, "Revolution Hacking," *Cyber War in Perspective: Russian Aggression against Ukraine,* edited by Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015): 56-7. New vulnerabilities came from zero-day exploits, which typically sell on the dark-web for only nation state values.

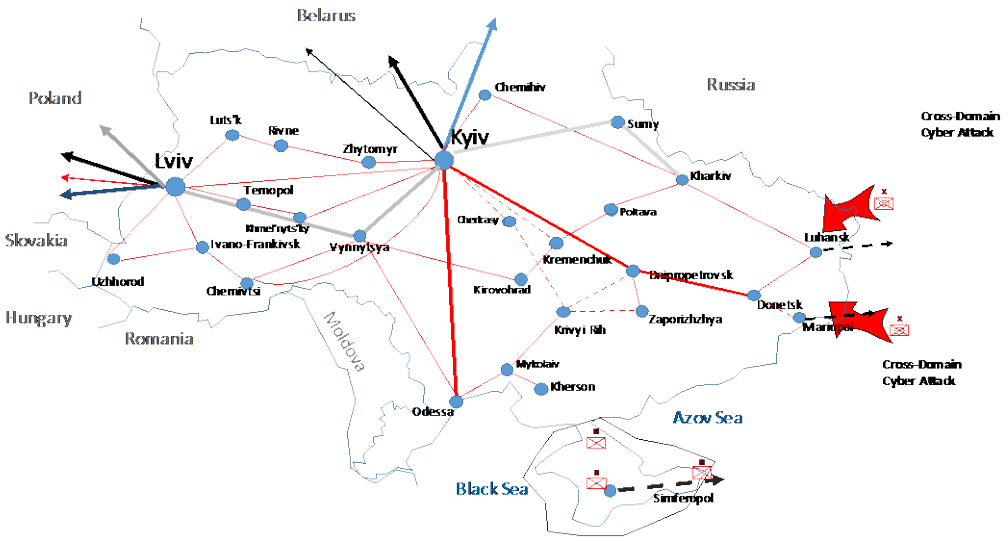

Figure 4.2. Cross Domain Attack in the Donbass. Campaign. Crimea and Donbass regions land maneuvers isolated cyberspace by controlling main fiber lines from the remainder of the Ukraine.

The sixth pulse, the Donbass invasion, began on July 2014, as the conflict shifted to the Don River region. Cyberspace played an increasingly important role in military operations. Multi-domain operations altered the logical terrain of cyberspace to the advantage of Russian interests.[125] (See Figure 4.2) Russian SIGINT, including cyber espionage, allowed for effective combat operations planning against the Ukrainian army with multi-domain sensors and cross-domain remote fire observation. Rerouted Ukrainian mobile traffic provided advanced forces protection and the operational reach to project defensive counter-attacks. Simultaneously, Russian forces provided support, assistance, and facilitation to Russian insurgents in the Donbass.

During the seventh pulse, pro-Russian forces enveloped through technological advantages of the Russian cyber, land, and air assets to isolate Ukrainian forces responding to the Donbass insurgency. However, the Ukrainian and Russian Presidents Poroshenko and Putin met. Poroshenko agreed to withdraw Ukrainian forces and established an effectively demilitarized zone in the

[125] Pakharenko, “Cyber Operations at Maidan,” 63.

Donbass. Only two days after the meeting on August 26, 2014, cyberattacks ceased. The eight pulse occurred on July 24, 2014, Ukraine accused Russia of arming pro-Russian separatists with tanks. The United States confirmed that multiple tanks crossed into Ukraine from Russia. Russian troops reinforced the Ukrainian border, and deployed additional heavy artillery enhanced by cyber capabilities.[126]

The ninth pulse shattered the operational tempo when the Ukraine for the Russian Federation became culminated by a chaotic sequence of events surrounding the destruction of Flight MH-17 (see Figure 4.3 ninth pulse). On July 17, 2014, pro-Russian separatists supplied by the Kremlin killed 298 people on Malaysian Airlines Flight MH-17 over the Donetsk, Ukraine with a surface to air missile.[127] International reaction quickly undercut the legitimacy of the Russian interests which soured by July 28, 2014 with the US Department of State release of photographic evidence that Russia integration included heavy artillery to pro-Russian forces.[128] International outcry resulted in escalating economic sanctions. Even on September 5, 2014 the expected ceasefire saw Ukrainian forces come under artillery fires while the Russian's retained influence over conflict

[126] Kahn and Beese, "FPI Fact Sheet," 3-4; William Mauldin, "U.S. Imposes Sanctions, Renews Concerns Over Russian Forces Near Ukraine," *The Wall Street Journal*, last modified June 20, 2014, last accessed October 1, 2016, http://www.wsj.com/articles/u-s-adds-ukrainian-separatists-to-sanctions-list-1403277646; Peter Baker, "Doubting Putin, Obama Prepares to Add Pressure," *The New York Times*, last modified June 24, 2014, last accessed October 1, 2014, http://www.nytimes.com/2014/06/25/world/europe/doubting-putin-obama-prepares-to-add-pressure.html.

[127] Jon Ostrower, Margaret Coker, Alexander Kolyandr, "Map of a Tragedy: How MH17 Came Apart Over Ukraine," *The Wall Street Journal*, last modified July 25, 2014, last accessed October 3, 2016, http://graphics.wsj.com/mh17-crash-map/; Jon Ostrower, Margaret Coker, Alexander Kolyandr, "After Flight 17 Crash, Agony, Debris and Heartbreak in Ukraine Villages," *The Wall Street Journal*, modified July 25, 2014, accessed October 2, 2014, http://www.wsj.com/articles/after-flight-17-crash-agony-debris-and-heartbreak-in-ukraine-villages-1406335532.

[128] Karen DeYoung, "U.S. releases images it says show Russia has fired artillery over border into Ukraine," *The Washington Post*, last modified July 27, 2014, last accessed October 3, 2014, https://www.washingtonpost.com/world/national-security/us-releases-images-it-says-show-russia-has-fired-artillery-over-border-into-ukraine/2014/07/27/f9190158-159d-11e4-9e3b-7f2f110c6265_story.html; Cable News Network, "Photographic evidence?" *CNN*, last modified July 24, 2014, last access October 3, 2016, http://www.cnn.com/interactive/2014/07/world/russia-ukraine-shelling-satellite-photos/.

outcomes in Donbass *oblasts* and massed soldiers on the border.[129] The nineth pulse led to intermediate strategic outcomes for the Russian Federation, September 5, negotiations resulted in the signing of the Minsk II protocols.[130] Cyber and land forces retracted from strategic objectives within their domains in Donbass. The Russian Federation had obtained its primary and secondary strategic objectives. NATO and EU limited expansion leaving the Russian Federation as the uncontested regional hegemon and Ukrainian resistance became internationally framed.

However, another isolated tenth pulse came as the Russian Federation demonstrated a burst cyber-attack for strategic interests. Minsk II provided an understanding between NATO and Russia to provide an intermediate Ukrainian solution. On December 23, 2014, after Ukrainian peace talks ended at Minsk II, a new cyber-attack expanded a paradigm shift for nation-states. The December cyber-attack derived from the same genetics of the November 2014 sample which the Ukrainian FSB had defeated. The Minsk II protocols did not force the Russian Federation from unplugging national assets that could still promote their strategic outcomes in 2015.

The Russian Federation Cyber, Land, Ukrainian and International Actions

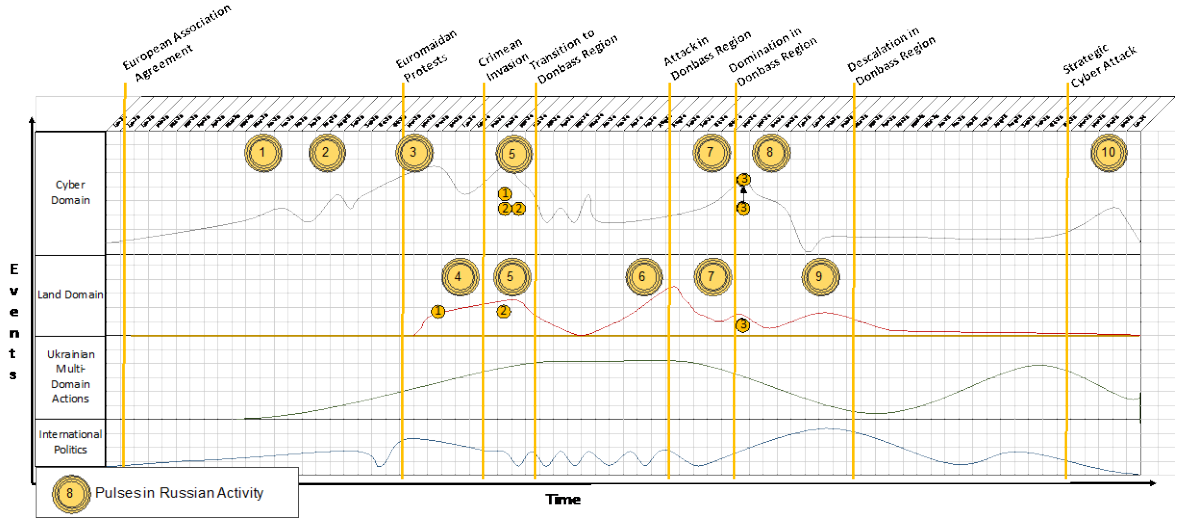

Figure 4.3. Land and Cyber Tempos. Pulses between domains and international events experienced by the Ukraine between 2013 to 2015.

[129] MacAskill and Walker, "Heavy shelling in Ukrainian," September 5, 2014.

[130] Thomas, *Russia Military Strategy*, 394.

The tenth pulse on December 23, 2015 was a cyber-attack that caused Ivano-Frankivsk region to lose power. Hundreds of thousands on Christmas eve were left in the freezing dark bringing all hospitals, water treatment, and economic systems to a standstill. The Ukrainian Kyivoblenergo, a regional electricity distribution company, reported the service outages to customers. The country's energy minister blamed Russia for the attack on the power grid. Security firm ESET agreed the malware known as BlackEnergy caused the outage and was a trojan malware attributional to the Russia Federation in previous attacks in the Donbass.[131] The outages were due to a third party's illegal entry into the company's computers and SCADA systems.[132] More important this event provides a sample of kinetic strategic cyber-attack outside the confines of synergistic cross-domain warfare.

The Russo-Ukrainian conflict between 2013 to 2015 provides four important key events orchestrated by the Russian Federation. January to September 2013 experienced an escalation of cyber-attack supporting analysis of events for political outcomes without land forces. Post-Euromaidan cyber forces shifted to amplifying the success of Crimean occupation by the Russian Federation ground forces. Escalation followed the cyber and land forces mutually supporting ethnic Russian separatists in Donbass region. Culmination occurred after cease fire accords because of political outcomes from the destruction of MH-17; the Russian Federation maintained cyber freedom of maneuver to achieve strategic outcomes demonstrated by the December 23 kinetic cyber-attack.

---

[131] Pakharenko, "Cyber Operations at Maidan," 63.

[132] Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *Defense Use Case* (Washington, DC: Electricity Information Sharing and Analysis Center (E-ISAC), March 18, 2016): *1*-8.

Findings

Alan Turning predicted that the complexity of the machine he created could not model the exact objective reality.[133] The interactions of cyber and land warfare required two hypotheses to be validated by the research questions. This study did not seek to precisely model the complex interactions between land and cyber domains. The study only tried to support the theory that the characteristics of cyberspace amplify the physical dynamics of cross-domain warfare regarding operational art. The findings of this study determined that the two hypotheses support the theory. First, the research questions indicate that land operations alter the state of cyberspace, and land power (or other domains) must be synchronized with cyber operations for operational reach. Second, the research questions support the hypothesis that cyber operations impact landpower and alter the available time, space and purpose of land warfare. Ultimately, like any complex adaptive system, human decision makers must refine specified heuristics to determine how best cross-domain cyber-land actions may best achieve strategic objectives.

The Russo-Ukrainian Conflict between 2013 and 2015 indicates that each of the research questions are valid. The characteristics of cyberspace extended operational reach within the cross-domain context. The infrastructure, nodes and logical ports of cyberspace were observed as transmutable by land forces. The logical structure and control from cyberspace impacted the operational reach of the Russian land forces. The case study also demonstrated that the synchronization of anticipated characteristics of cyberspace impact joint tempo through frequency, duration, and sequencing that create options in cross-domain warfare. Cyber power in isolation often can only maintain temporal dominance for short durations until the opponent adapts. The cyber domain also can preserve and amplify the tempo of other domains as observed in both the Crimea and the Donbass.

---

[133] Turing, "Computing Machinery and Intelligence," 455.

The first hypothesis states that if land operations alter the state of cyberspace, then landpower (or other domains) must be synchronized with cyber operations to extend operational reach. The evidence from the case suggests that the first hypothesis is supported. Observations of cyber warfare from the key events in the Russo-Ukrainian conflict demonstrate how cyber power manipulates the available time, space and purpose of land warfare. Command and control isolation contributed to the lethargic response by the leadership of the Ukraine and led to further cyber exploitation. Indication in the case study provides two events that demonstrate the cyber alteration from land activities. First, Crimea operations placed logical cyberspace into the rear area of the Russian cyber domain preventing and protecting land forces which seized the peninsula. In the Donbass region, cyber enabled maneuver, targeting, and mass of land fires through land manipulations. Finally, the Russo-Ukrainian study demonstrates the harmony of cyber and land operations juxtaposed against pre-Maidan and post-Minsk environments.

The dependence of commanders on the space to make decisions and employ forces in time can be operationally shocked by the cyber domain. The resulting paralysis throughout the entire depth of the opponent's battle area enables land forces to isolate, penetrate, and exploit events on the ground. Further, the study demonstrated how land maneuvers could perform the same effects to enable cyber activities. Cyberspace closed the temporal distances for land maneuvers. Land forces secured key points of cyber-topography and extended duration of control in cyberspace to dominate the operational environment.

Russo-Ukrainian (2013-2015) Actor Operational Tempos

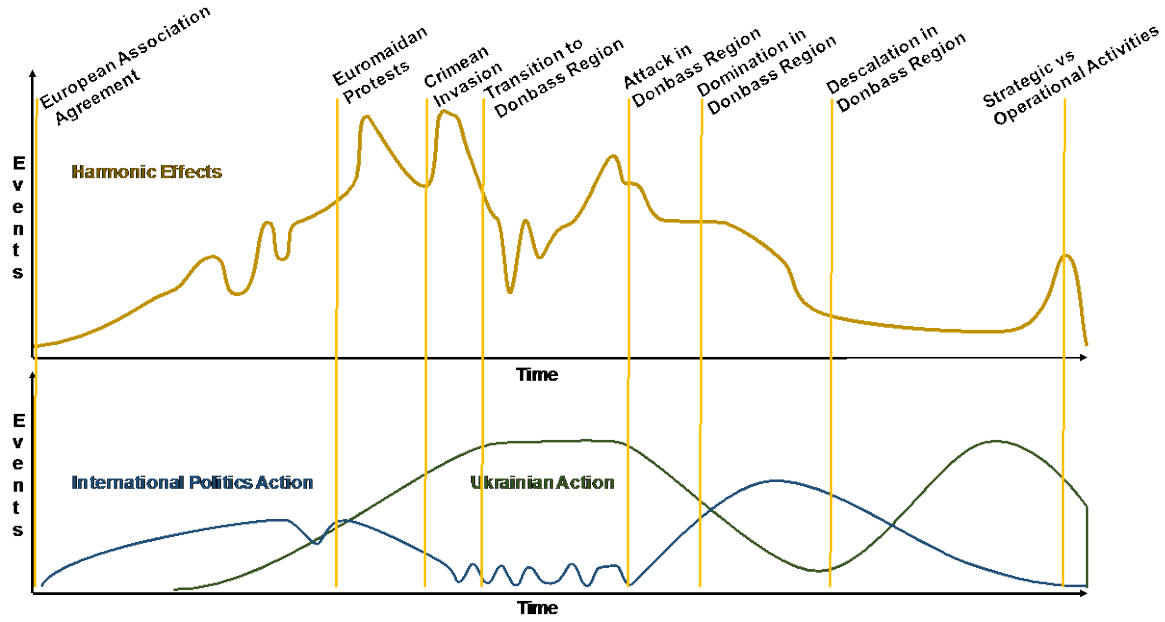

Figure 5.1. Cross-Domain Tempo. The Russo-Ukrainian conflict tempos 2013 to 2015.

The second hypothesis states that if cyber operations impact landpower, then cyberspace can alter the available time, space and purpose of land warfare. The evidence of the case study also supports this hypothesis. The characteristics of cyberspace change the effects of landpower. The nature of complex adaptive systems leaves the progenitor of the system able to predict the desired function within the confines of the root design but incapable of understanding the shifting system due to catalysts external to the system. The duration of catalytic events and the shift in frequencies indicate an interdependence between domains.

The Russian Cyber, Land, Cross-Domain actions with Ukrainian and International Actions in Time between 2013 to 2015.

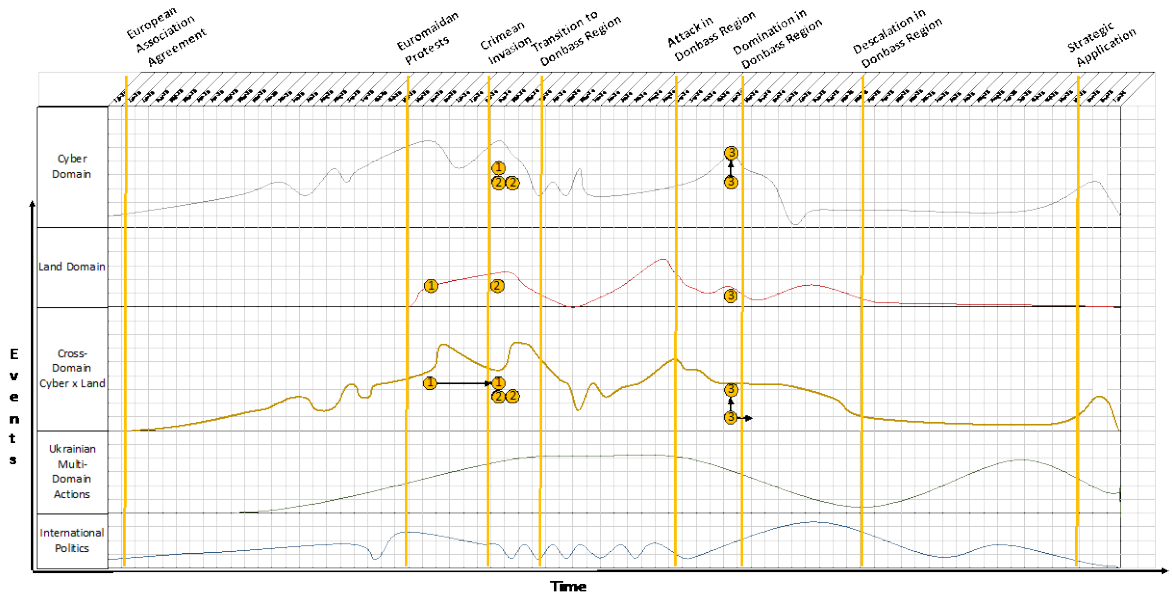

Figure 5.2. Land and Cyber Domain Tempo of Pulses 2013-2015. The interrelated cross-domain tempo as experienced by the Ukraine between 2013 to 2015.

The relationship between domains depends on the context of the cyber architecture and mechanism employed in the theater of war. The Russian Federation designed and contributed to the Ukrainian information architecture and military capabilities before 2013. The evidence indicates cyberspace provided an operational maneuver corridor into the Ukrainian OODA loop. Land actions separate from cyber means spiked periods of culmination and action. However, cyber amplification of land forces occurred as the land forces altered the topography of cyberspace. Further, the marked contrast between events observed between November 2014 and February 2015 within the electrical grid attack on December 24, 2015, indicate the rapid culmination of cyber without the support of the land domain. Clearly, the evidence suggests a strong connection between the cyber domain and actions made in other domains.

The Ukrainian case study provides clear evidence that land operations synchronized with cyber during the Crimean campaign dissected Ukrainian sovereignty interests. Further, the Donbass campaign demonstrates a constant struggle to align cross-domain objectives by land forces to dominate cyber infrastructures that lead to potential asymmetrical advantages. Also, Donbass

indicates the mutual amplification of effects preventing culmination in either cyber or land domains. The absence of land power during December 24, 2014, indicted a risk for cyber warfare as a strategic arm of political objective sans cross-domain warfare which could quickly culminate without external influences.

Conclusions

This study sought to determine the potential interaction of cyber to the application of operational art in Joint Warfare. The identified characteristics of cyberspace have the ability to alter the employment of operational art as a result of the physical dynamics of cross domain warfare. The two hypotheses this study evaluated support this thesis. First, if cyber operations impact land power, then cyberspace can alter the available time, space and purpose of land warfare. Second, if land operations modify the state of cyberspace, then land power (or other domains) must be synchronized with cyber operations for operational reach.

This case study utilized a structured focused approach to evaluating a theory that application of cyberspaces' characteristics and operational art establish processes of critical intersections (key events) of a cyber-land domain activity.[134] The study provided evidence that the characteristics of cyberspace provide greater options to operational artists because of cross-domain linkages in warfare. The case study evaluated Russian Federation cyber operations in time and space to support a theory that cyber and land force actions can transform mutual operational reach. Further, the study employed modeling of observed interactions which indicate synchronous land and cyber power change the construct of the operational art regarding tempo to transform the time, space and purpose for strategic aims.

Russo-Ukrainian New Generation Warfare 2013-2015

[134] George and Bennett, *Case Studies and Theory*, 69.

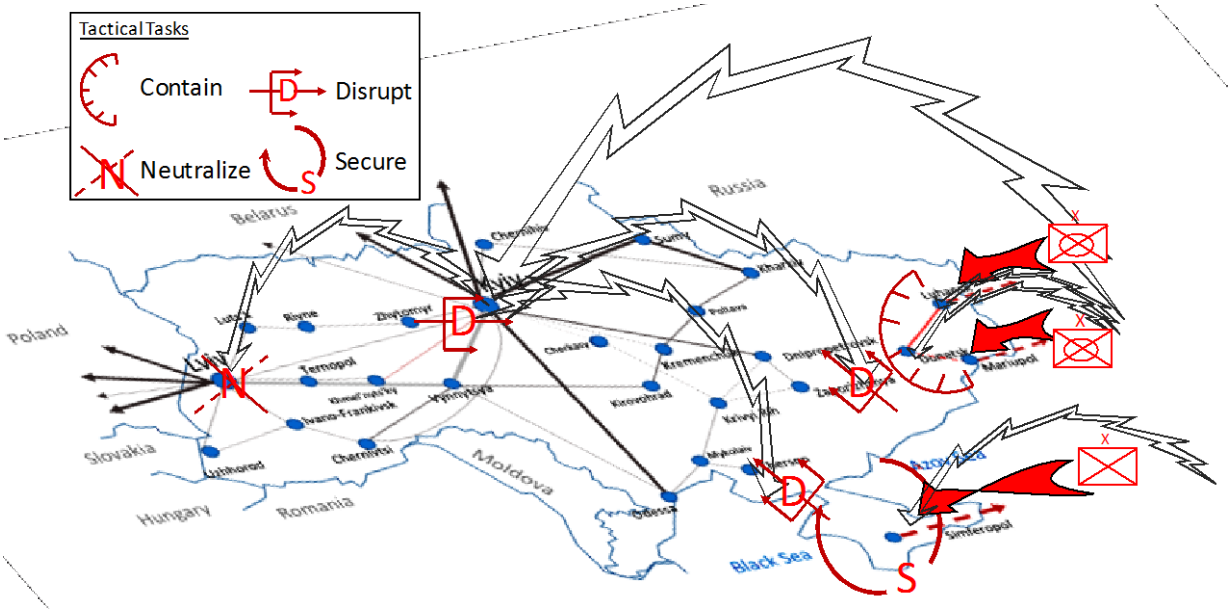

Figure 6.1. New Generation Warfare. Interpretation of the Russo-Crimean Conflict 2013-2015. Cyber forces disrupt land forces from Kiev to the Crimea and the Donbass. Airborne and Spetsnaz secure the Crimea in all domains. The Russian land forces support pro-Russian rebels in Luhansk and Donetsk through isolating the Donbass cyberspace, irregular forces, air-defense, and field artillery. Finally, cyber-attacks to neutralize the western Ukraine electrical grid extend operational outcomes.

The Joint application of symbiotic relationships between cyber requires synchronization across all domains. The Ukrainian case study supports the hypothesis that land operations synchronized with cyber achieved a synergy that altered the operational reach. The study observations indicated that the design of activities could align cross-domain objectives by ground forces to dominate. Also, Donbass events showed the mutual amplification of effects preventing culmination in either cyber or land domains. The kinetic cyberattack observed on December 24, 2015, indicates the rapid culmination of cyber without cross-domain interaction. The study supports the validity of cyber characteristics. The observed changes in operational reach and tempo provide evidence to the body of military theory that cross-domain synthesis that answers the standard questions and supports the hypotheses.

Military leaders employing cross-domain warfare must consider employment that synchronizes the characteristics of cyberspace with other domains. Cross-domain warfare requires

more than simultaneity of multi-domain war. The study indicates a complex interaction between cyber and land that theoretically can extend between all other domains of warfare. The study supports military theory seeking solutions to domain offsets and asymmetric approaches. The characteristics and observations in the case study provide a new framework for aggressive strategies employing cyber with cross-domain operations to meet strategic outcomes.

The study presents a critical analysis for warfighters, strategists, and political leaders. Military warfighters must develop a concept of the operational environment, including cyber, and the potential cross-domain effects. The strategist must understand the environmental potential, enemy capabilities, and friendly force potential influenced by cross-domain actions enabled by cyber to formulate menus of options. Political leadership must accept the range, speed, and transformation potential of cyberspace indicated in this study's findings.

Future studies should evaluate cross-domain integration between all domains simultaneously. An investigation into the behavior of cross-domain warfare affecting complex change with all domains would support of enhance the known characteristics o cyberspace proposed by the research. also, research validating the strategic impact of cyber warfare employed to isolate strategic assets in time would enhance understanding toward planning Time Phased Force Deployment and other synchronous mobilizations. Any research should come from exploring how the new machine created by and after Turing and others has changed the operational and strategic actions which assume methods of controlling physical systems. After all the new system, according to Turing, cannot be understood by the same system trying to understand it.

Bibliography

Books

Axelrod, Robert and Michael D. Cohen. *Harnessing Complexity: Organizational Implications of a Scientific Frontier.* New York: Basic Books, 2000.

Bousquet, Antoine. *The Scientific War of Warfare: Order and Chaos on Battlefields of Modernity.* New York: Columbia University Press, 2009.

Boyne, Walter J. *The Influence of Air Power Upon History.* New York: K. S. Ginger Company, 2003.

Bundiansky, Stephen. *Air Power: The Men, Machines, and Ideas That Revolutionized War, From Kitty Hawk to Iraq.* New York: Penguin Books, 2005.

Carr, Jeffery. *Inside Cyber Warfare.* Cambridge, MA: O'Reilly Media Inc., 2012.

Cebrowski, A. K. *Implementation of Net-Centric Warfare.* Washington, DC: Office of Force Transformation, January 5, 2005.

Clarke, Richard A. and Robert K. Knake, *Cyber War,* New York: HarperCollins, 2010.

Clausewitz, Carl Von. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Corbett, Julian S. *Principles of Maritime Strategy.* Mineola, NY: Dover Publications, 2004.

Dolman, Everett Carl. *Pure Strategy: Power and Principle in the Space and Information Age*. New York: Routledge, 2005.

Echevarria, Antulio J. II. "American Operational Art, 1917-2008," *Evolution of Operational Art*. Edited by John Andreas Olsen and Martin Van Creveld. New York: Oxford University Press, 2011.

Gat, Azar. *A History of Military Thought: From the Enlightment to the Cold War.* New York: Oxford University Press, 2001.

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

Harrison, Richard W. *Architect of Soviet Victory in World War II.* Jefferson, NC: McFarland & Company, 2010.

Isserson, Georgii Samoilovich. *The Evolution of Operational Art.* Translated by Bruce W. Menning. Fort Leavenworth, KS: Combat Studies Institute Press, 2013.

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

Levy, Steven. *hackers: heroes of the computer revolution.* Sebastopol, CA: O'Reilly Books, 2010.

Libicki, Martin C. *What Is Information Warfare*, Washington, DC: US Government Printing Office, August, 1995.

Lind, Williams S. *Maneuver Warfare Handbook.* Boulder, CO: West View Press, 1985.

Klein, John J. *Space Warfare: Strategy, Principles and Policy.* New York: Routeldge, 2006.

Mahan, A. T. *The Influence of Sea Power Upon History 1660-1783.* New York: Dover Publications Inc., 1987.

National Defense Research Institute, *Networks and Netwars: The Future of Terror, Crime, and Militancy*. edited by John Arquilla and David Ronfeldt. Washington, DC: National Defense Research Institute, 2001.

Naveh, Shimon. *In Pursuit of Military Excellence: The Evolution of Military Theory*. New York: Frank Cass Publishers, 1997.

Osinga, Frans P. B. *Science, Strategy and War: The Strategic Theory of John Boyd.* New York: Routledge, 2007.

Thomas, Timothy L. *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*. Fort Leavenworth, KS: Foreign Military Studies Office (FMSO), 2015.

Articles

Aron, Leon. "The Putin Doctrine: Russia's Quest to Rebuild the Soviet State." *Foreign Affairs* (March 8, 2013). Accessed October 16, 2016. https://www.foreignaffairs.com/articles/russian-federation/2013-03-08/putin-doctrine.

Applegate, Scott D. "The Principle of Maneuver in Cyber Operations," *4th International Conference on Cyber Conflict* (2012): 183-195.

Boyd, John R. "Destruction and Creation." Unpublished Paper. September 3 1976. Retrieved from http://dnipogo.org/john-r-boyd/.

Chekinov, S. G. and S. A. Bogdanov. "The Nature and Content of a New–Generation War." *Voennaya Mysl': Military Thought*, no. 10 (2013):13-25.

Citino, Robert. "'*Die Gedanken sid* frei': The Intelectual Culture of the Interwar German Army," *The Army Doctrine and Training Bulletin* 4, no. 3 (Fall 2001): 48-55.

Darczewska, Jolanta. "The Devil Is In The Details: Information Warfare In The Light Of Russia's Military Doctrine." *OSW Point of View*, no. 50 (May 2015).

De Czege, Huba Wass. "Thinking and Acting Like an Early Explorer: Operational Art is not a Level of War." *Small Wars Journal*. Last modified March 14, 2011. Accessed August 12, 2016. http://www.smallwarsjournal.com/blog/journal/docs-temp/719-deczege.

Gerasimov, Valery. “The Value of Science Is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.” *Voyenno-Promyshlennyy Kuryer Online* (February 26, 2013). Translated by Robert Coalson, June 24, 2014. Accessed September 29, 2016. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

Gerasimov, Valery. “The Value of Science in Prediction: New Challenges Require Rethinking on the Forms and Methods of Warfare.” *Military Review* (January-February 2016): 23-9. Accessed August 30, 2016. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

Giles, Keir. “Russia and Its Neighbours: Old Attitudes, New Capabilities.” *Cyber War in Perspective: Russian Aggression against Ukraine.* Edited by Kenneth Geers. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Gjelten, Tom. “FIRST STRIKE: US Cyber Warriors Seize the Offensive,” *World Affairs* 175, no. 5 (January/February 2013): 33-43.

Godfrey, M.D. and D.F. Hendry. “The Computer as von Neumann Planned It,” *IEEE Annals of the History of Computing* 15, no. 1 (1993).

Gray, Colin S. “Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling.” *Strategic Studies Institute Monograph* (April, 2013): 8-45.

Kelly, Sanja et al. “Freedom on the Net 2014.” *Freedom on the Net.* Freedom House (2014).

Martin-Vegue, Tony. “Are we witnessing a cyber war between Russia and Ukraine? Don’t blink – you might miss it,” *Cyber Security Online.* Last modified April 24, 2014. Accessed August 17, 2016. http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html.

Mc Granahan, William J. “The Fall and Rise of Marshal Tukhachevsky.” *Parameters* 8, no. 4. Carlisle Barracks, PA: Army War College, 1978: 62-72.

Miller, Matthew, Jon Brickey, and Gregory Conti. “Why Your Intuition About Cyber Warfare is Probably Wrong,” *Small Wars Journal* (November 29, 2012). Accessed October 3, 2016. http://www.smallwarsjournal.com/printpdf/13573.

Moore, Gordon E. “Cramming More Components Onto Integrated Circuits.” *Electronics* 38, *no. 8* (April 19, 1965).

Motyl, Alexander J. “The Sources of Russian Conduct.” *Foreign Affairs* (November 16, 2014). Accessed August 30, 2016. https://www.foreignaffairs.com/articles/russian-federation/2014-11-16/sources-russian-conduct.

Norman, Douglas O. and Michael L. Kuras. “Engineering Complex Systems.” *Selected Readings D300: Army Design Methodology AY 2011-1.* Fort Leavenworth, KS: School of Advanced Military Studies, 2011.

Perry, Brett. “Non-liner Warfare in Ukraine: The Critical Role of Information Operations and Special Operations.” *Small Wars Journal* (August 14, 2015). Accessed August 30, 2016. http://smallwarsjournal.com/printpdf/27014.

Rid, Thomas and John Arqulla. “Think Again: Cyberwar.” *Foreign Policy,* no. 192 (March/April 2012): 80-4.

Rivera, Jason. “Has Russia Begun Offensive Cyberspace Operations in Crimea?” *Georgetown Security Studies Review* (March 2, 2014) http://georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea/.

Schreier, Fred . “On Cyberwarfare,” *DCAF Horizon 2015 Working Paper, no. 7*. Geneva, Switzerland: Geneva Centre for Democratic Control of Armed Forces, 2015.

Snegovaya, Maria. “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare.” *Russia Report I*. Washington, DC: Institute for the Study of War, September 2015.

Starodubtsev, Yu. I, V. V. Bukharin, and S. S. Semyonov. “Technosphere Warfare.” *Voennaya Mysl’ (Military Thought), no. 7* (2012): 22-31.

Turing, Alan M. “Computing Machinery and Intelligence,” *Mind New Series* 59, *no. 236.* Oxford University Press, October 1950. 433-460.

Unwala, Azhar and Shaheen Ghori, “Brandishing the Cybered Bear: Informaion War and the Russia-Ukraine Conflict,” *Military Cyber Affairs* 1, art 7. Tampa Bay, Florida: Scholar Commons, 2015.

Wihl, Lloyd, Maneesh Varshney, and Jiejun Kong. "Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments," *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) Paper, no. 10313.* Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), 2010.

Reports

Alberts, David S. and Richard E. Hayes. *Power to the Edge.* Washington, DC: DoD Command and Control Research Program, June 2003.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. “W32.Stuxnet Dossier: Version 1.4,” *Symantec Security Response Report.* February, 2011.

General Accounting Office (GAO). “GAO/NSIAD-97-134 Operation Desert Storm Air Campaign.” *Report to the Ranking Minority Member, Committee on Commerce, House of Representatives.* Washington, DC: US General Accounting Office, June 1997.

Giles, Keir. “The Next Phase of Russian Information Warfare.” *Report*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, May 20, 2016.

Hinsley, Sir Harry. “The Influence of ULTRA in the Second World War,” *Security Group Seminar.* Cambridge, United Kingdom: Babbage Lecture Theater Computer Laboratory, Cambridge University, November 26, 1996.

iSight. “Russian Cyber Espionage Campaign – Sandworm Team,” *iSight Partners* (2014).

Lee, Robert M., Michael J. Assante, and Tim Conway. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” *Defense Use Case*. Washington, DC: Electricity Information Sharing and Analysis Center (E-ISAC), March 18, 2016.

Lewis, Jason. “Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare.” *LookingGlass Cyber Threat Intelligence Group.* Baltimore, MD: LookingGlass Cyber Solutions, April 28, 2015.

Liles, Samuel et al. “Applying Traditional Military Principles to Cyber Warfare,” *2012 4th International Conference on Cyber Conflict.* Tallinn, Estonia: NATO CCD COE Publication, 2012.

Kahn, Tzvi and Evan Beese. “FPI Fact Sheet: Timeline of Russian Aggression in Ukraine and the Western Response.” Washington, DC: The Foreign Policy Initiative, September 18, 2014.

Kamoun, Farouk. “Hierarchical Routing Procedures for Large Computing Networks,” *Design Considerations for Large Computer Communication Networks, ARPA CONTRACT No DAHC-15-73-C-0368.* Los Angeles, California: School of Engineering and Applied Sciences, University of California, April, 1976.

Kleinrock, Leonard et al. “Computer Network Research.” *Advanced Research Projects Agency Semiannual Technical Report.* Los Angeles: School of Engineering and Applied Sciences, University of California, June 30, 1972.

Kleinrock, Leonard et al. “Computer Network Research.” *Advanced Research Projects Agency Semiannual Technical Report.* Los Angeles: School of Engineering and Applied Sciences, University of California, December 31, 1973.

Koval, Nikolay. “Revolution Hacking.” *Cyber War in Perspective: Russian Aggression against Ukraine.* Edited by Kenneth Geers. (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015).

North Atlantic Treaty Organization. “Analysis of Russia’s Information Campaign Against Ukraine: Examining Non-Military Aspects of the Crisis in Ukraine from a Strategic Communications Perspective.” *Report.* Riga, Latvia: NATO StratCom Centre of Excellence, December 1, 2016..

Tukhachevskii, M.N. “New Issues of War: Новые вопросы войны,” *Voenno-Istoicheskii Zhurnal, no. 2* (1962): 73-5 quoted by Naveh, Shimon. *In Pursuit of Military Excellence: The Evolution of Military Theory.* New York: Frank Cass Publishers, 1997.

Doctrine

Army Doctrine Reference Publication 5-0. *The Operations Process.* Washington, DC: Government Printing Office, 2012.

Dempsey, GEN Martin E. "Forward," *Joint Operational Access Concept (JOAC) v 1.0*. Washington, DC: Government Printing Office, 2012.

Fleet Marine Force Reference Publication (FMFRP) 3-201. *Spetsnaz.* Washington DC: Department of the Navy, January 18, 1991. Accessed March 10, 2015. http://cnqzu.com/library/Anarchy%20Folder/Military%20Reference%20and%20History/Spetsnaz%20-%20FMFRM%203-201.pdf.

The Russian Federation Ministry of Defense. "Information Security Doctrine of the Russian Federation" (2008). Accessed August 30, 2016. http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

Joint Publication 3-0. *Joint Operations.* Washington, DC: Government Printing Office, August 11, 2011.

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

Joint Publication 3-14. *Space Operations*. Washington, DC: Government Printing Office, 2013.

Lind, Williams S. *Maneuver Warfare Handbook.* Boulder, CO: West View Press, 1985.

Kem, BG John S. to the Army University, August 15, 2016. *Topics for Consideration by SAMS, CGSC and Other Students for MMAS and Other Degree Program/Requirements*. Fort Leavenworth, KS: US Command and General Staff College, 2016.

Obama, Barack, White House. "Statement by the President on Ukraine." February 28, 2014. Accessed October 2, 2016. https://www.whitehouse.gov/the-press-office/2014/02/28/statement-president-ukraine.

US Department of Defense. *The Department of Defense Cyber Strategy*. Washington, DC: Office of the Secretary of Defense, April 2015.

Webpages

Agence France-Presse. "Hackers Target Ukraine's Election Website." *Agence France-Presse*. October 25, 2014. Accessed October 15, 2016. http://www.securityweek.com/hackers- target-ukraines-election-website.

Arbor Networks. "Digital Attack Map." *Arbor Networks*. August 25, 2014. Accessed October16, 2016. http://www.digitalattackmap.com/v1#anim=1&color=0&country=ALL&list=1&time=16306&view=map.

———. “Digital Attack Map.” *Arbor Networks*. July 26, 2014, Accessed October15, 2016, http://www.digitalattackmap.com/v1#anim=1&color=0&country=ALL&list=0&time=16247&view=map.

Baker, Peter. “Doubting Putin, Obama Prepares to Add Pressure.” *The New York Times*. June 24, 2014. Accessed October 1, 2014. http://www.nytimes.com/2014/06/25/world/europe/doubting-putin-obama-prepares-to-add-pressure.html.

Balmforth, Richard and Dmitry Zhdannikov. “UPDATE 1-Ukraine signs landmark $10 bln shale gas deal with Shell.” *Reuters*. January 24, 2013. Accessed October 15, 2016. http://www.reuters.com/article/shale-ukraine-idUSL6N0ATER320130124.

“Ukraine PM Mykola Azarov warns of coup in making.” *BBC*. December 2, 2013. Accessed October 15, 2016. http://www.bbc.com/news/world-europe-25192792.

———. “Crimea referendum: Voters ‘back Russia union’.” *BBC*. March 16, 2014. Accessed October 2, 2016. http://www.bbc.com/news/world-europe-26606097.

———. “Ukraine crisis in maps.” *BBC*. February 18, 2015. Accessed October 1, 2016. http://www.bbc.com/news/world-europe-27308526.

———. “Putin: Russia helped Yanukovych to flee Ukraine.” *BBC*. October 24, 2014. Accessed October 16, 2016. http://www.bbc.com/news/world-europe-29761799.

Berners-Lee, Tim. "The Original HTTP as defined in 1991." *World Wide Web Consortium (W3C), 1991*. Accessed 01 September 2016. http://www.w3.org/Protocols/HTTP/AsImplemented.html.

Cable News Network. “Photographic evidence?” *CNN*. July 24, 2014. Accessed October 3, 2016. http://www.cnn.com/interactive/2014/07/world/russia-ukraine-shelling-satellite-photos/.

Coker, Margaret and Paul Sonne. “Cyberwar’s Hottest Front.” *The Wall Street Journal*. 10 November 2015.

Cyber Security Online. April 24, 2016. Accessed August17, 2016. http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html.

DeYoung, Karen. “U.S. releases images it says show Russia has fired artillery over border into Ukraine.” *The Washington Post*. July 27, 2014. Accessed October 3, 2014. https://www.washingtonpost.com/world/national-security/us-releases-images-it-says-show-russia-has-fired-artillery-over-border-into-ukraine/2014/07/27/f9190158-159d-11e4-9e3b-7f2f110c6265_story.html.

“Cyberwar: War in the fifth domain.” *The Economist: Briefing*. Last modified July 1, 2010. Access August 17, 2016. http://www.economist.com/node/16478792.

European Research Council. “Ukraine Fiber Optic Line.” Last modified 2015. Accessed October 21, 2016. http://infrastructure.kiev.ua/upload/Fiber.png.

Finn, Peter. “Putin Threatens Ukraine On NATO.” *The Washington Post.* February 13, 2008. Accessed October 16, 2016. http://www.washingtonpost.com/wp-dyn/content/article/2008/02/12/AR2008021201658.html.

Berners-Lee, Timothy. "The Original HTTP as defined in 1991." *World Wide Web Consortium (W3C),* 1991. Accessed September 01, 2016. http://www.w3.org/Protocols/HTTP/AsImplemented.htm

MacAskill, Ewen and Shaun Walker. “Heavy shelling in Ukrainian port of Mariupol hours before agreed ceasefire.” *The Guardian.* September 5, 2014. Accessed October 3, 2014. https://www.theguardian.com/world/2014/sep/05/ukraine-heavy-shelling-hours-before-ceasefire-russia.

Malkin, G. “Internet Users’ Glossary,” *Request For Comment (RFC) 1392.* Edited by T. LaQuey Parker. Last modified January, 1993. Accessed August 17, 2016. https://tools.ietf.org/html/rfc1392.

Mauldin, William. “U.S. Imposes Sanctions, Renews Concerns Over Russian Forces Near Ukraine.” *The Wall Street Journal*. June 20, 2014. Accessed October 1, 2016. http://www.wsj.com/articles/u-s-adds-ukrainian-separatists-to-sanctions-list-1403277646

Myers, Steven Lee and Alison Smale. “Russian Troops Mass at Border With Ukraine.” *The New York Times*. March 13, 2014. Accessed October 1, 2016. http://www.nytimes.com/2014/03/14/world/europe/ukraine.html?_r=1.

“Feb. 28 Updates on the Crisis in Ukraine,” *The New York Times: The Lede*. February 28, 2014. Accessed October 1, 2016. http://thelede.blogs.nytimes.com/2014/02/28/latest-updates-tensions-in-ukraine/.

Ostrower, Jon, Margaret Coker, Alexander Kolyandr. “After Flight 17 Crash, Agony, Debris and Heartbreak in Ukraine Villages.” *The Wall Street Journal.* July 25, 2014. Accessed October 2, 2014. http://www.wsj.com/articles/after-flight-17-crash-agony-debris-and-heartbreak-in-ukraine-villages-1406335532.

———. “Map of a Tragedy: How MH17 Came Apart Over Ukraine.” *The Wall Street Journal.* July 25, 2014. Accessed October 3, 2016. http://graphics.wsj.com/mh17-crash-map/.

Pancevski, Slovyansk Bojan. “Putin’s 300 whip up Ukrainian turmoil.” *The Sunday Times.* April 27, 2014. Accessed October 1, 2016. http://www.thesundaytimes.co.uk/sto/news/world_news/Ukraine/article1404493.ece.

“Ukraine says communications hit, MPs phones blocked.” *Reuters*. March 4, 2014, http://www.reuters.com/article/2014/03/04/ ukraine-crisis-cybersecurity-idUSL6N0M12CF20140304.

———. “Timeline: Political crisis in Ukraine and Russia’s Occupation of Crimea.” *Reuters*. March 8, 2014. Accessed October 1, 2016. http://www.reuters.com/article/us-ukraine-crisis-timeline-idUSBREA270PO20140308.

Network Working Group. *Request for Comments: 1122 (RFC 1122).* Network Working Group, Internet Engineering Task Force, October 1989. Edited by R. Braden. Accessed July 29, 2016. https://tools.ietf.org/html/rfc1122#section-1.1.2.

Ryan, Rosalind. “Join NATO and we’ll target missiles at Kiev, Putin wans Ukraine.” *Reuters.* February 12, 2008. Accessed October 15, 2016. https://www.theguardian.com/world/2008/feb/12/russia.ukraine.

Taylor, Adam. “‘Novorossiy,’ the latest historical concept to worry about in Ukraine.” *The Washington Post*. April 18, 2014. Accessed October 3, 2016. https://www.washingtonpost.com/news/worldviews/wp/2014/04/18/understanding-novorossiya-the-latest-historical-concept-to-get-worried-about-in-ukraine/.

Taylor, Adam. “That time Ukraine tried to join NATO – and NATO said no.” *The Washington Post.* September 4, 2014. Accessed October 15, 2016. https://www.washingtonpost.com/news/worldviews/wp/2014/09/04/that-time-ukraine-tried-to-join-nato-and-nato-said-no/.

Ukretelcom. “Ukrtelecom’s Crimean sub-branches officially report that unknown people have seized several telecommunications nodes in the Crimea.” Last modified February 28, 2014. Accessed October 1, 2016. http://en.ukrtelecom.ua/about/news?id=120467.

Watson, Ivan and Maxim Tkachenko. “Russia, Ukraine agree on naval-base-for-gas deal.” *CNN.com.* April 21, 2010. Accessed October 15, 2016. http://www.cnn.com/2010/WORLD/europe/04/21/russia.ukraine/index.html?hpt=T2#.

Zamakis, Petro. “Cyber Wars: The Invisible Front.” *Ukraine Investigation*, April 24, 2014. accessed October 15, 2016. http://ukraineinvestigation.com/cyber- wars-invisible-front/.

Monographs

Anderson, Talon. “Adapting Unconventional Warfare Doctrine to Cyberspace Operations: An Examination of Hacktivist Based Insurgencies.” Monograph, US Army Command and General Staff College, 2015.

Converse, Bradley D. “Cyber Power and Operational Art: A Comparative analysis with air power,” Master’s Thesis. Newport, RI: Naval War College, 2013.