ARMY SPECIAL OPERATIONS IN INFORMATION ADVANTAGE

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

MASTER OF MILITARY ART AND SCIENCE
Information Advantage Scholars

by

ANDREW L. FALKENSTINE, MAJOR, US ARMY
B.S. Criminal Justice, Sam Houston State University, Huntsville, Texas, 2011

Fort Leavenworth, Kansas
2022

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-06-2022	Master's Thesis	AUG 2021 – JUN 2022

4. TITLE AND SUBTITLE

Army Special Operations in Information Advantage

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Andrew L. Falkenstine

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States is shifting focus towards strategic competition with China and Russia. In competition, the US must look for ways to gain advantages by prioritizing the gaining of and exploiting advantages in the information environment. China and Russia have prioritized and shown a willingness to incorporate actions that lead to an information advantage in recent operations. Yet, for all the talk, the US is lagging in the competition for an information advantage. This study finds that China and Russia value creating an information advantage but go about it in completely different manners. China seeks to influence through diplomatic and economic means to build a coalition to support its global endeavors. While Russia thrives in chaos and seeks to stoke it and exploit it to its advantage. This thesis examines how the US can narrow this information advantage gap using Army Special Operations Forces (ARSOF) and this study provides a few recommendations on how to leverage these uniquely trained forces that can contribute to the US gaining an advantage in a strategic competition against China and Russia.

15. SUBJECT TERMS

Information Advantage; Strategic Competition; Army Special Operations;

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER *(include area code)*
(U)	(U)	(U)	(U)	106	

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

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Andrew L. Falkenstine

Thesis Title: Army Special Operations in Information Advantage

Approved by:

_____, Thesis Committee Chair
Trent J. Lythgoe, Ph.D.

_____, Member
Brian L. Steed, Ph.D.

_____, Member
Monique G. Guerrero, M.S.

_____, Member
LTC Christopher M. Baldwin, M.A.

Accepted this 10th day of June 2022 by:

_____, Assistant Dean of Academics for
Dale F. Spurlin, Ph.D. Degree Programs and Research

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

ABSTRACT

ARMY SPECIAL OPERATIONS IN INFORMATION ADVANTAGE, by Andrew Falkenstine, 106 pages.

The United States is shifting focus towards strategic competition with China and Russia. In competition, the US must look for ways to gain advantages by prioritizing the gaining of and exploiting advantages in the information environment. China and Russia have prioritized and shown a willingness to incorporate actions that lead to an information advantage in recent operations. Yet, for all the talk, the US is lagging in the competition for an information advantage. This study finds that China and Russia value creating an information advantage but go about it in completely different manners. China seeks to influence through diplomatic and economic means to build a coalition to support its global endeavors, while Russia thrives in chaos and seeks to stoke it and exploit it to its advantage. This thesis examines how the US can narrow this information advantage gap using Army Special Operations Forces (ARSOF) and this study provides a few recommendations on how to leverage these uniquely trained forces that can contribute to the US gaining an advantage in a strategic competition against China and Russia.

ACKNOWLEDGMENTS

I want to take the time to acknowledge the many people that allowed me to get this research from where it started, to where it is today. First, I want to thank Dr. Lythgoe my committee chair, who patiently assisted me throughout the process by putting structure and rigor to my incoherent thoughts. To the rest of my committee, you all provided invaluable insights along the way that helped to guide my research and recommendations. I appreciate your guidance collectively and individually.

I would like to acknowledge Mr. Chris Johnson and fellow classmate Brian Graham, whom both took my broad ideas in A221 and helped to focus them down with timely and constructive feedback. They were the first to provide me with feedback and helped to shape my research when I was struggling to find the right scope and framework on which to base my research. I would also like to thank Mr. Peter Im, my instructor in the information advantage scholars' program, his perspectives, and tireless work ethic helped to frame my research and ensure that it is relevant to the Army Special Operations community.

Finally, I would like to thank my family, my wife Kimberlee and three kids Kyran, Pepper, and Christian. While they were not always happy about it, they always provided me the time and support to do the research required to successfully complete this.

TABLE OF CONTENTS

Page

ACRONYMS

AI	Artificial Intelligence
ARSOF	Army Special Operations Forces
BRI	Belt Road Initiative
CA	Civil Affairs
EW	Electromagnetic Warfare
ML	Machine Learning
NATO	North Atlantic Treaty Organization
OAIs	Operations, Activities, and Investments
PSYOP	Psychological Operations
SF	Special Forces
SIGINT	Signals Intelligence
SOCOM	Special Operations Command
USASOC	United States Army Special Operations Command

ILLUSTRATIONS

TABLES

Page

CHAPTER 1

INTRODUCTION

Background

> The Army is embracing a new era characterized by the accelerating growth of information, information sources, and information dissemination capabilities supported by information technology. This new era, the so-called Information Age, offers unique opportunities as well as some formidable challenges.
>
> –Headquarters, Department of the Army,
> Field Manual 100-6, *Information Operations*

Creating conditions that give an advantage over the adversary is a fundamental principle of traditional warfare but is even more prevalent and complex in the competitive environment of today.[1] Advantages for the military comes in many forms and ranges from a numerical or capability advantage to a geographic or psychological advantage.[2] Advantage is inherently relative to your competitor and can be fleeting as they have a vote in how they respond to that advantage or as external circumstances change, so advantages must be capitalized on when achieved.[3] Simply having an advantage in a specific area does not translate to overall success, and using that

[1] Robert Leonhard, *The Principles of War for the Information Age* (New York: Ballentine Books, 1998), 54.

[2] Christopher Paul, "Understanding and Pursing Information Advantage," *Cyber Defense Review* 5, no. 2 (Summer 2020): 112, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Paul_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053231-950#:~:text=A%20position%20of%20relative%20advantage%20is%20a%20location,risk%20and%20move%20to%20a%20position%20of%20disadvantage.

[3] Ibid., 113-114.

advantage to exploit the adversary's weakness is only a means to accomplish the objective.[4]

Information in the context of warfare and creating an advantage over the adversary is broad and can be ambiguous. However, information is at the root of all advantages, as it enables or inhibits a Commander's situational awareness, command and control, and can be used to influence behaviors of the adversary or third-party actors that can affect the overall objective.[5] As such, any type of advantage that is sought in the competition space must be closely tied to gaining and exploiting an information advantage over the competition.

Strategic competitors China and Russia have proven themselves willing and effective at leveraging information-related capabilities to gain advantages over the US across the strategic framework of Diplomatic, Information, Military, and Economic (DIME). According to the 2018 National Defense Strategy, China and Russia are utilizing emerging technology to influence neighboring countries and coerce those who oppose them, to build themselves up as a global power.[6] China sees creating information dominance as a prerequisite for all joint operations to "paralyze enemy operational

---

[4] Paul, "Understanding and Pursing Information Advantage," 115.

[5] Ibid., 119.

[6] Robert J. Bebber, "Treating Information as a Strategic Resource to Win the 'Information Warfare'," *Orbis* 61, no. 3 (2017): 394-403, https://www.sciencedirect.com/science/article/abs/pii/S0030438717300492?via%3Dihub; Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (Spring 2018): 105-122, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf.

system of systems" and "sabotage the enemy's war command system of systems."[7] Concurrently, Russia seeks to undermine democratic countries in its sphere of influence to discredit them while expanding its own information capabilities.[8] Russia has a long history of information warfare and it is an important part of its efforts to preserve Putin's regime and to establish Russia as a global power.[9]

The US has not dealt with an adversary with the technical competence, capability, and ambition as they are currently with China and Russia.[10] The US military must find new approaches to shorten the Observe, Orient, Decide, Act (OODA) loop to give decision-makers the information advantage over China and Russia.[11] Information advantage must be prioritized across all operations as its effects extend beyond the scope of any one mission. Failure to do this will have strategic consequences by giving strategic

[7] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 117.

[8] Secretary of Defense, *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[9] Deborah Yarsike Ball, "Protecting Falsehoods with a Bodyguard of Lies: Putin's Use of Information Warfare," (Research Paper No. 136, Research Division, NATO Defense College, Rome, February 2017), 1-2, https://www.ndc.nato.int/news/news.php?icode=1017.

[10] Keith Alexander and Jamil Jaffer, "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition," *Georgetown Journal of International Affairs* 19 (Fall 2018): 51-52, http://www.jstor.org/stable/26567527.

[11] Scott McIntosh, "The Wingman-Philosopher of MiG Alley: John Boyd and the OODA Loop," *Air Power History* 58, no. 4 (Winter 2011): 24, https://www-jstor-org.jsou.idm.oclc.org/stable/26276108.

competitors an advantage over the US, as this will allow them to enable its decision-makers.

The US military has been the dominant force across the globe since the end of the Cold War, which changed the way adversaries view the US and how to compete against them and developed what foreign policy expert David Kilcullen calls "conceptual envelopment."[12] This is where the concept of war is expanded, leading to two different outcomes. First, the adversary acts in a way that it deems war but does not meet the threshold of war for the US, and by the time the US realizes it is at war, it is already behind. Second, which can be even more dangerous, is that the US thinks it is acting in the competition space, but the adversary believes that the US is committing aggressive acts of war. Either way, both sides misunderstanding the other side's intentions can be disastrous for US objectives[13]

The US Army is currently focused on multi-domain operations alongside the joint force to provide decision-makers with options to defeat the enemy while creating dilemmas for the adversary to create physical and psychological advantages.[14] The US military has invested in its cyberspace capability, electromagnetic warfare, intelligence, and psychological operations to gain an information advantage over its adversaries.[15]

---

[12] David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York, NY: Oxford University Press, 2020), 175.

[13] Ibid., 176.

[14] Andrew Feickert, "Defense Primer: Army Multi-Domain Operations (MDO)," (Congressional Research Service, Washington, DC, updated October 22, 2021), https://sgp.fas.org/crs/natsec/IF11409.pdf.

[15] Ibid.

However, the US is facing new challenges from China and Russia in the competition for information advantage.

Although the US has devoted significant assets to developing tools in the information environment to compete with China and Russia, the US must continue to prioritize and find innovative ways to compete in an evolving and complex information environment. The US military has a resource that can contribute to gaining an advantage over strategic competitors in the Army Special Operations Forces (ARSOF). These forces are specially trained across a wide array of core competencies to include training foreign partners, cultivating military-civilian relationships, influencing foreign audiences, and are already conducting operations worldwide against other threats, working with US government agencies and partner nation forces. As the competition space intensifies, ARSOF can be used to help shape the environment either independently, or with partner nations in countries that are being threatened by strategic competitors.[16] This does two things: it assures the US stays partners of choice over China and Russia, and working in these countries allows the US to observe adversarial networks and enable US decision-makers on ways to better target and disrupt Chinese and Russian threat activities.[17]

[16] Stephen Watts, Sean M. Zeigler, Kimberly Jackson, Caitlin McCulloch, Joseph Cheravitch, and Marta Kepe, *Countering Russia: The Role of Special Operations Forces in Strategic Competition* (Santa Monica, CA: Rand Corporation, 2021), 34, https://www.rand.org/pubs/research_reports/RRA412-1.html.

[17] Ibid., 49.

Problem Statement

Strategic competitors China and Russia continue to expand their capabilities to gain and exploit an information advantage and exploit US limitations. This is important because if the US fails to sufficiently prioritize and innovate how it leverages information, it will be competing at a relative disadvantage.

Purpose of the Study

The purpose of this study is to gain a better understanding of why China and Russia are successfully competing in the information environment by examining Chinese and Russian information operations and to examine the best opportunities for the US to create an information advantage and identify the capabilities best situated to take advantage of those opportunities. This study's findings will lead to recommendations for ARSOF developing ways that can mitigate China and Russia's strengths, while also exploiting their weaknesses, giving the US a relevant advantage in the information environment.

Research Questions

Primary Research Question

How can the US Army Special Operations Forces contribute to gaining an information advantage over China and Russia?

Secondary Research Questions

1. What are strategic competitors China and Russia's current views on information advantage?

2. What have strategic competitors China and Russia recently done to create an information advantage?

Assumptions

This study makes three assumptions:

1. China and Russia are attempting to gain an information advantage over the United States by operating in regions that hold strategic importance.

2. Current Chinese and Russian ability to create and disrupt effects in the information environment outweigh the US in terms of scale, but not necessarily in capability.

3. All sources used to better understand Chinese and Russian capabilities have been translated correctly and represent their true capabilities and not used to deceive the US.

Definition of Terms

Information Advantage: "is a condition when a force holds the initiative in terms of relevant actor behavior, situational understanding, and decision making through the use of information."[18]

[18] Michael Hammerstrom, "Delivering the Information Advantage," (PowerPoint Presentation, TechNet, Cyber Center of Excellence, Augusta, GA, 2021), 3, https://events.afcea.org/Augusta21/Custom/Handout/Speaker0_Session8922_1.pdf.

Operational Environment: "A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[19]

Information Environment: *"*The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command-and-control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information.*"*[20]

Narrative: *"*A narrative is an organizing framework expressed in story-like form. Narratives are central to representing identity, particularly the collective identity of religious sects, ethnic groupings, and tribal elements. They provide a basis for interpreting information, experiences, and the behavior and intentions of other individuals and communities. Stories about a community's history provide models of how actions

[19] Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Washington, DC: Joint Chiefs of Staff, 2018, GL-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/docnet/jp30/story_content/external_files/jp3_0_20170117%20(1).pdf.

[20] Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Washington, DC: Joint Chiefs of Staff, 2014), IX-X, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

and consequences are linked. Thus, narratives shape decision making in two ways: they provide an interpretive framework for a complicated and uncertain environment and offer idealized historical analogies that can serve as the basis for strategies. ”[21]

Scope

This study examines Chinese, and Russian operations, activities, and investments (OAIs) within the construct of the five lines of effort for information advantage:

1. “Enable decision making.” [22]

2. “Protect friendly information.”[23]

3. “Inform domestic and foreign audiences.”[24]

4. “Influence foreign audiences.”[25]

5. “Conduct information warfare.”[26]

These five lines of effort will be assessed by looking at China and Russia’s strengths and weaknesses for each of these lines of effort.[27] This analysis will provide a better

[21] Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-24, *Counterinsurgency* (Washington, DC: Joint Chiefs of Staff, 2018), xi, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_24.pdf.

[22] Hammerstrom, “Delivering the Information Advantage,” 2.

[23] Hammerstrom, “Delivering the Information Advantage,” 2.

[24] Hammerstrom, “Delivering the Information Advantage,” 2.

[25] Hammerstrom, “Delivering the Information Advantage,” 2.

[26] Hammerstrom, “Delivering the Information Advantage,” 2.

[27] Dac Teoli, Terrence Sanvictores, and Jason An, “SWOT Analysis,” National Center for Biotechnology Information, National Lirary of Medicine, last updated September 08, 2021, https://www.ncbi.nlm.nih.gov/books/NBK537302/.

understanding of China and Russia's strengths and weaknesses on creating information advantage. It will then recommend how ARSOF can contribute to information advantage against these strategic competitors. This research will only examine capabilities and technology that are currently available to ARSOF and strategic competitors.

Limitations and Delimitations

Limitations

Due to time and financial constraints, all data and sources used for this research are from the Combined Arms Research Library and online sources.

Delimitations

This study will be limited to English language documents. Where Chinese and Russian documents are used, the research will rely on English translations. This study only examines Chinese and Russian actions that are related to their use of the five lines of effort of information advantage across the DIME spectrum. This research will be limited to publicly available unclassified information to maximize the reading audience of the research. While the author acknowledges current events involving Russia in Ukraine, those events are not within the timeframe of this research. Recommendations made because of this research are generic to avoid compromising ongoing operations.

Summary

This chapter shows how having an information advantage encapsulates a broad range of advantages and its relevancy to the competition environment. It illustrates that China and Russia are continuing to expand their ability to create a relative advantage over

the US in the information environment.[28] This indicates why the US must prioritize and leverage its capabilities to stay competitive in the information environment.

[28] Mark Pomerleau, "Why Is the United States Losing the Information War?" *C4ISRNet*, October 05, 2020, https://www.c4isrnet.com/information-warfare/2020/10/05/why-is-the-united-states-losing-the-information-war/.

CHAPTER 2

LITERATURE REVIEW

Introduction

> The essence of maneuver is taking action to generate and exploit some kind of advantage over the enemy as a means of accomplishing our objectives as effectively as possible.
>
> –U.S. Marine Corps, Marine Corps Doctrinal Publication 1, *Warfighting*

This chapter begins by reviewing thoughts on information and information warfare and how it has evolved over time. Next, it examines how China and Russia view, prioritize, and utilize information to their advantage, especially when it comes to competing with the US. Finally, this chapter explores how the US has viewed information operations and identifies a gap of the US Army and ARSOF specifically trying to shift from the global war on terrorism (GWOT) to strategic competition, and its struggle to evolve and contribute to information advantage for the US and shape the environment prior to conflict as it was designed to do.

Information Warfare and the Information Environment

The term information is a word that can mean many different things depending on how it is used. Merriam-Webster defines information as "knowledge obtained from investigation, study, or instruction," hence the adage that "knowledge is power."[29] That power can be conveyed through hard and soft means; hard power is the ability to force others to do something in your favor they would otherwise not do, and soft power is the

[29] Merriam-Webster, Incorporated, "Information," Merriam-Webster, accessed April 11, 2022, https://www.merriam-webster.com/dictionary/information.

ability to get others to want to do something that is beneficial to you through attraction rather than coercion.[30]

Information has been used as a source of power throughout the history of warfare to create an advantage over an adversary, with Genghis Khan as an early example.[31] Khan is known as a great conqueror who utilized barbaric methods throughout his conquest of the known world in the 13th century.[32] Khan leveraged his savage reputation to gain a psychological advantage over cities he was looking to conquer by sending runners ahead of his army to request the city to surrender or die.[33] Khan would then treat those who surrendered well, which further helped to persuade future cities to acquiesce to his demands.[34]

The importance of information in warfare has been discussed amongst military theorists since the days of Sun Tzu. The most common theme was on the psychological aspects of warfare and how to break the enemies' will and cause the enemy to lose hope without having to fight while instilling confidence in your own army to make them

---

[30] Robert Keohane and Joseph Nye Jr., "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (September-October 1998): 81-94, https://www-jstor-org.jsou.idm.oclc.org/stable/20049052?seq=6.

[31] John Bokel, "Information as an Instrument and a Source of National Power," (Paper, The Industrial College of the Armed Forces, National Defense University, Fort McNair, Wasington, DC, 2003), 2, https://apps.dtic.mil/sti/pdfs/ADA422060.pdf.

[32] Frank McLynn, "The Brutal Brilliance of Chengis Khan," *History Extra*, February 22, 2019, https://www.historyextra.com/period/medieval/the-brutal-brilliance-of-genghis-khan/.

[33] Ibid.

[34] Ibid.

resilient to any attempts by the enemy to do the same to you.[35] Sun Tzu said, "to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."[36] Flavius Vegetius Renatus stated that "the courage of the soldier is heightened by the knowledge of his profession. A courageous soldier is less susceptible to intimidation by the enemy."[37] A second concept discussed just as much is the use of deception to gain an advantage and the importance of protecting friendly information. B.H. Liddell Hart argued that "Deception can then directly contribute to the achievement of surprise and indirectly to security and economy of effort as stated in the present description of the term." Clausewitz did not believe deception to be an effective instrument in warfare and had little strategic value, but that "surprise is an independent element that has the psychological effect of gaining superiority. Surprise is produced by speed and secrecy."[38] Napoleon placed great importance on protecting information to ensure his plans remained secret, he exercised centralized command and limited the number of people who knew the plans, which sped

[35] Arto Hirvelä, "Thoughts of War Theorists on Information Operations," (Paper presented at European Conference on Information Warfare & Security, Helsinki, Finland, 2011), 127, https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/detail/detail?vid=2&sid=540fdbd3-73e0-4d33-ab6b-88dffdefd4d3%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=67467530&db=tsh.

[36] Ibid., 128.

[37] Ibid.

[38] Ibid., 130.

up the decision-making process and minimized the ability of the enemy to discover his plans, giving Napoleon the advantage of surprise.[39]

The aim of information by historical military theorists was focused primarily on the adversary or creating effects on the battlefield, however, as the ability to communicate grows, so do the number of uses for which information is used to inform and influence to gain and exploit advantages in and out of a battle. As technology expands, so too does the ability for actors to wield information as an instrument of power and blur the lines between strategic, operational, and tactical levels of warfare.[40] This is evidenced recently by the Islamic State leveraging social media to amplify tactical-level events to a global audience which gave them operational and strategic effects and affected national and global policies on the use of technology moving forward.[41]

As information technology advances, so does the ability to propagate information. Going back to the US civil war, the use of the telegraph changed the speed in which information could travel across the battlefield. For the first time, information could be sent instantaneously from the front lines to supporting elements, this enabled

---

[39] Hirvelä, "Thoughts of War Theorists on Information Operations," 129.

[40] Norman Davis, "An Information-based Revolution in Military Affairs," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla, and David Ronfeldt (Washington, DC: Rand Corporation, 1997), 86, https://www.jstor.org/stable/10.7249/mr880osd-rc.9?seq=1.

[41] P. W. Singer and Emerson Brooking, *Like War: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt Publishing Company, 2018), 232-238; Brian Steed, . "Narrative as a Critical Component for Violent Weaker Actor Success," (Ph.D. diss., University of Missouri-Kansas City, 2020), 157-158, https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/74002/Steed_umkc_0134D_11583.pdf?sequence=1.

commanders to rapidly receive and send information, speeding up command and control and mobilization of military resources.[42] However, this also allowed for reporters to send news back to the civilian population which brought about a lot of misinformation and commanders deciding to censor or ban what they were allowed to send.[43] From the early 1900s through World War II, there were many advancements in radio technology that enabled commanders to increase their reach without sacrificing time, or command and control.[44] The ability to increase radio frequencies and the capacity to use radios inside of tanks enabled Col. Heinz Guderian of the German army to develop and use the theory of blitzkrieg in Germany's rush across Europe.[45] The increase in civilian radio use also allowed for the proliferation of propaganda for both sides to bolster the confidence of the civilian population while degrading the morale and deceiving the enemy.[46] Since the end of the second world war, the US has prioritized its research and design program for the military which has led to advancements in information technology that eventually made

[42] Yael A. Sternhell. "Communicating War: The Culture of Information in Richmond during the American Civil War," *Past & Present*, no. 202 (February 2009): 183, http://www.jstor.org/stable/25580922.

[43] Ibid., 184.

[44] Karl Larew, "From Pigeons to Crystals: The Development of Radio Communication in US Army Tanks in World War II," *Historian* 67, no. 4 (2005): 665, https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=6&sid=1294c4c9-9a21-4ff7-b300-a49b19f31f2b%40redis.

[45] Ibid., 666.

[46] K.R.M. Short, *Film and Radio Propaganda in World War II* (Knoxville: University of Tennessee Press, 1983), 3.

up the components that led to the creation of the internet as it is known today.[47] This along with other advances in technology led to the US having technological overmatch that it enjoyed in the Gulf War, which in turn changed the course of information warfare and how competitors viewed the US and it how it would counter US superiority.

Chinese Information Advantage

China in its effort of becoming the global superpower has closely studied fellow strategic competitors, the United States and Russia, especially in the information environment. China desires to understand competitor's capabilities better to blend US and Russian techniques with their concepts to create a uniquely Chinese approach.[48] By the mid-2000s, China developed its doctrine focusing on psychological warfare as an extension of information warfare.[49] While the Chinese examined both US and Russian doctrine and warfare, China sees the US as its main competition.[50]

The Chinese aim is to offset what they perceive as US advantages in the information domain. Until the 1990s, the Chinese military took a primarily defensive posture in the information domain, but this changed after the 1991 Gulf War between the

[47] Kira Fabrizio and David Mowery, "Defense-Related R&D and the Growth of the Postwar Information Technology Industrial Complex in the United States," *Revue d'économie industrielle* 112, no. 4 (2005): 27, https://www.persee.fr/doc/rei_0154-3229_2005_num_112_1_3123.

[48] Christopher Paul, James Dobbins, Scott W. Harold, Howard J. Shatz, Rand Waltzman, and Lauren Skrabala, *A Guide to Extreme Competition with China* (Santa Monica, CA: Rand Corporation, 2021), 9, https://www.rand.org/pubs/research_reports/RRA1378-1.html.

[49] Ibid., 23.

[50] Kilcullen, *The Dragons and the Snakes*, 25.

United States and Iraq.[51] China witnessed the rapid and total domination of Iraq's Command, Control, Communications, Computers (C4) Intelligence, Surveillance, and Reconnaissance (ISR) (C4ISR) systems by the US and its partners. The Chinese realized they could not compete with Western information capabilities. China began analyzing US military doctrine to understand how to compete with the US in the information domain.[52] This analysis led them to conclude that the Gulf War was a high watermark for the United States. The Chinese believe that the US is obsessed with war and high-tech weaponry and that the overwhelming victory in the Gulf War has given the US a false sense of superiority.[53] In addition to modernizing their doctrine to fight the US, senior Chinese military leaders worked to develop an unrestricted warfare concept to compete against the US.

To better understand the Chinese way of thinking when it comes to how they seek to gain an information advantage, it is important to understand the concept of unrestricted warfare as it is applied across all Chinese concepts of warfare.[54] As a part of unrestricted warfare, the Chinese have created the Side-Principal rule, which is derived from the basic Chinese grammar concept of the center word and the modifier.[55] The side-principal is

---

[51] Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: Strategic Sudies Institute and U.S. Army War College Press, March 2014), 26, https://publications.armywarcollege.edu/pubs/2263.pdf.

[52] Ibid., 27.

[53] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Panama City, Panama: Pan American Publishing, 1999), x.

[54] Ibid., ix.

[55] Ibid., 133.

asymmetrical in structure and used to maximize one's strengths, which causes the side element to dictate the direction of the principal element.[56] The side-principal applies to all global actors, as no country's resources are limitless, it must efficiently allocate its resources, not directly against the opponent's strengths or weaknesses, but in a way that takes advantage of its resources in the best way to achieve its objectives [57] In the current environment, with lines being blurred and inherently more complex, a military-on-military fight may not be the best use of one's resources, and the answer may even be outside of the military complex.[58]

The second concept of unrestricted warfare that is important for understanding how China goes about information advantage is the Chinese idea of "going beyond limits" or boundaries by fair or foul means to accomplish their objectives.[59] This does not always mean going to the extreme in everything done but being willing to go outside international law and norms to achieve the objective is encouraged as a way of thinking.[60] This concept has eight principles:

1. Omnidirectionality: Where you combine the use of all available resources to ensure no blind spots and have maximum situational awareness.

[56] Liang and Xiangsui, *Unrestricted Warfare,* 136.

[57] Ibid., 142.

[58] Ibid., 144.

[59] Ibid., 154.

[60] Ibid., 171.

2. Synchrony: Military and non-military forces working together shrinks the overall battlefield and accomplishes multiple objectives simultaneously.

3. Limited objectives: Limited objectives will allow for accomplishment, if the first objective is too grand, it will lead to disastrous results.

4. Unlimited measures: Free employment and creativity of actions to accomplish the limited objectives prescribed.

5. Asymmetry: This allows one to be proactive and take advantage of one's strengths while leveraging the adversary's abilities against themselves.

6. Minimal consumption: Objectives are concise and straightforward to avoid waste of resources on efforts that distract from the overall objective.

7. Multidimensional coordination: Considers many non-military and non-war factors in planning as it relates to accomplishing a specific objective.

8. Adjustment and control of the entire process: Conditions change and must be continually evaluated to adjust actions as necessary.[61]

As future conflicts will be borderless, crossing into multiple domains relying on military might alone will not be possible. One must consider all factors on the modern battlefield while adhering to the above principles. These principles do not guarantee victory but violating them assuredly leads to defeat and is evident in the way China conducts operations in the information environment.[62]

[61] Liang and Xiangsui, *Unrestricted Warfare*, 177-185.

[62] Ibid., 190.

China has elevated itself on the global stage without ever going to war but by utilizing information warfare against competitors' leaders and populations.[63] China seeks to fight asymmetrically through three types of information warfare: public opinion warfare, legal warfare, and psychological warfare.[64] The Chinese view public opinion (or media) warfare to bolster the confidence of its own population while influencing competitors' perceptions of China. This is done through many types of propaganda efforts to emphasize the strengths of China while downplaying or denying its weaknesses. The Chinese believe that whichever side gets the information out to the public first has an advantage; this includes using deception tactics as a part of their dissemination plan. China is proactive in securing the initiative to increase the likelihood of creating a shift in opinion in its favor. A second way China wages public opinion warfare is to control domestic media and what is presented to the public as a counter to Western media, even going as far as punishing and silencing dissenting views.[65] Legal warfare for China gives them justification for any physical actions before they take place. China looks for legal loopholes that it can work around or exploit against the competition.[66] Psychological warfare for China is key to gaining an information

[63] Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Backgrounder No. 2821, The Heritage Foundation, Washington, DC, 2013), 1, https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

[64] Ibid., 1-4.

[65] Ibid., 5-9.

[66] Paul et al., *A Guide to Extreme Competition with China*, 23.

advantage over its competition. It has broken psychological warfare down into five broad tasks:

1. Presenting one's own side as just and thus the competition as unjust.

2. Emphasizing one's advantage which will boost internal confidence while simultaneously influencing your competition's perceptions.

3. Undermining the opposition's will to resist by degrading their morale and isolating them from their sources of support.

4. Encouraging dissension in the opponent's camp which plays off the last task by causing the opponent to become weary of the fight and call to cease operations.

5. Implement psychological defenses against the opponents' attempts at psychological warfare for both protection of your own, and to also expose and exploit failed attempts by the opposition.[67]

China's doctrine and thoughts on information warfare are evident in its strategic guidance to the People's Liberation Army (PLA) which nests its operations under three concepts: active defense, local war, and people's war.[68] Active defense posture going back to the days of Mao Zedong, where they would only attack if attacked.[69] Local war is where China believes that future warfare will be conducted via advanced computer

[67] Cheng, "Winning Without Fighting," 4-5.

[68] Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2011* (Washington, DC: Department of Defense, 2011), 9, https://dod.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf.

[69] Ibid., 22.

systems and place an emphasis on network-centric warfare and information technology.[70] People's War is the utilization of the Chinese population to support the military in a time of war. This support can come in many forms, including logistical, political, operational, and civil defense.[71] Larry Wortzel, commissioner of the US-China economic and security review commission wrote,

> The truly distinguishing characteristic of operations in the information age in PLA doctrine, however, is that "information power and various types of firepower are merged" so that mobility and precision fires are integrated to increase their operational effects. Ultimately, the PLA must execute integrated operations combining computer network warfare, networked firepower warfare, electronic warfare, and sensor systems.[72]

China believes that the ability to gain superiority in physical domains such as air, land, and sea depends upon their ability to gain information superiority, which in part relies on superiority in cyberspace.[73] China views the ability to dominate cyberspace will set them up for success in the information domain and, thereby the operational environment.

Coinciding with Chinese modernization efforts for the military operating in the information environment, China engages in the information environment through its

---

[70] Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2011,* 3.

[71] Peng Guangoian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing: National Military Science Publishing House, 2005), 376.

[72] Wortzel, *The Chinese People's Liberation Army and Information Warfare,* 8.

[73] Herb Lin, "A Hypothetical Command Vision Statement for a Fictional PLA Cyber Command," *Cybersecurity and Deterrence* (blog), *Lawfare,* October 22, 2021, https://wwww.lawfareblog.com/hypothetical-command-vision-statement-fictional-pla-cyber-command.

economic investments with local governments worldwide.[74] China leverages their *Belt Road Initiative (BRI)* to gain access to countries to gain influence with them.[75] China can sell these infrastructure projects in developing countries as China helping these countries when no one else is helping, especially the US. This gives China an advantage to gain further inroads creating China as a partner of choice. This gives them an advantage over the US because they can out-spend the US in these countries, giving them a position of influence over that country as will be evidenced in the case study.

In summary, China seeks to become the predominant global power and views the US as its main impediment to accomplishing this goal. To compete with the US, China has studied strategic competitors and developed new ways of warfare. China sees the information domain as the primary domain that it can create advantages against the US and has utilized its resources to develop its capacity to operate in this space.

Russian Information Advantage

> Information warfare is a new form of battle of two or more sides which consists of the goal-oriented use of special means and methods of influencing the enemy's information resource, and also of protecting one's own information resource, in order to achieve assigned goals. An information resource is understood to be information which is gathered and stored during the development of science, practical human activity and the operation of special organizations or devices for the collection, processing and presentation of information saved magnetically or

[74] Jason Gambill, "China and Russia Are Waging Irregular Warfare Against the United States: It Is Time for a US Global Response, Led by Special Operations Command," Joint Intermediate Force Capabilities Office, November 15, 2021, https://jnlwp.defense.gov/Press-Room/In-The-News/Article/2857039/china-and-russia-are-waging-irregular-warfare-against-the-united-states-it-is-t/.

[75] Andrew McBride and James Chatzky, "China's Massive Belt and Road Initiative," Council on Foreign Relations, last updated January 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

> in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing or management tasks.[76]

Russia has a long history of conducting disinformation warfare to achieve its strategic objectives and has invested in its information capabilities to keep up with technology advancements to perpetuate its disinformation.[77] Russia is the first major power to make deception a part of its national policies, and its roots can be traced to the 18th century with Catherine the Great.[78] Disinformation has been predominant across Russia's history and Stalin in 1952 even went as far as trying to create a disinformation campaign to make it look like the concept of disinformation was a French concept to attack and weaken the Soviet bloc.[79] Russia has shown its willingness to employ these capabilities, from their efforts to forge documents to put Western powers in a bad light during the Cold War to their well-known efforts recently to influence other countries' elections through cyber means.[80] Russia works to circumvent international law by conducting operations through proxy forces, wielding indirect influence over opponents

---

[76] Timothy Thomas, "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," *The Journal of Slavic Military Studies* 11, no. 1 (March 1998): 40-62.

[77] Ion Mihai Pacepa and Ronald J. Rychlak, *Disinformation* (Washington, DC: WND Books, Inc., 2013), ii.

[78] Ibid., 37.

[79] Ibid., 39.

[80] Latvian Institute of International Affairs, *Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016), 7, https://stratcomcoe.org/publications/internet-trolling-as-a-hybrid-warfare-tool-the-case-of-latvia/160.

by supporting their opposition, employing strict control over information in its own country, and continually pushing the boundary of norms in the information domain.[81]

Many believe that Russia's greatest damage to the West was the intelligence operations that helped them build the atomic bomb, but Romanian Lt Gen Pacepa who is the highest-ranked military officer to defect from the eastern bloc, argues that it is in fact Russia's ability to change the past and frame events in a more favorable light to Russia.[82] Russia was able to transform the perception of Stalin in the eyes of some people from a dictator that killed over 20 million innocent civilians to a respected leader who ruled over one-third of the world and changed the perception of many other communistic dictators in the same light.[83] Russia used disinformation campaigns to portray many of those put to death as traitors to the country. Russia has done so well at reframing the past that it is increasingly harder for outside entities to unravel the truth from disinformation.[84]

In 2013, Russian General Staff and deputy defense minister Valeriy Gerasimov wrote an article on future war, which later became known as the Gerasimov doctrine, which foreshadowed what was to happen in Crimea in 2014.[85] In this article, he argued that the previous color revolution, Arab Spring, and operations in Iraq and Afghanistan illustrated a new and emerging way to achieving political-military goals, citing a need to

---

[81] Latvian Institute of International Affairs, *Internet Trolling as a Hybrid Warfare Tool,* 157-158.

[82] Pacepa and Rychlak, *Disinformation,* 44.

[83] Ibid.

[84] Ibid., 45.

[85] Ibid., 161.

include non-military measures such as diplomatic and economic means as a part of war. Gerasimov emphasized the importance of creating an advantage through pre-conflict shaping, which allows one's intentions to remain masked as long as possible, rapidly seize objectives, consolidate gains, and then quickly de-escalate, allowing for negotiation from a position of strength, this allows Russia to undermine adversaries politically and militarily.[86]

Building off the Gerasimov doctrine, David Kilcullen presents a theory for the Russian way of warfare described as *liminal warfare*. This concept describes Russian contemporary thinking on warfare and lends to the way Russia seeks to create advantages over Western powers through the use of information.[87] Liminal comes from the Latin word for threshold, which is used to describe the ambiguity of societies that are transitioning and can also refer to borders that are fuzzy and ambiguous up close.[88] Liminal warfare exploits this ambiguity, "it is neither fully overt nor truly clandestine; rather, it rides the edge, surfing the threshold of detectability, sometimes subliminal (literally 'below the threshold' of perception), at other times breaking fully into the open to seize an advantage or consolidate gains before adversaries can react."[89]

---

[86] Pacepa and Rychlak, *Disinformation*, 164.

[87] Kilcullen, *The Dragons and the Snakes*, 116.

[88] Ibid., 119.

[89] Ibid.

Liminal warfare begins at the detection threshold, it is ambiguous and shifts depending on the type of activity, which shows the range of maneuver space for liminal warfare in figure 1.

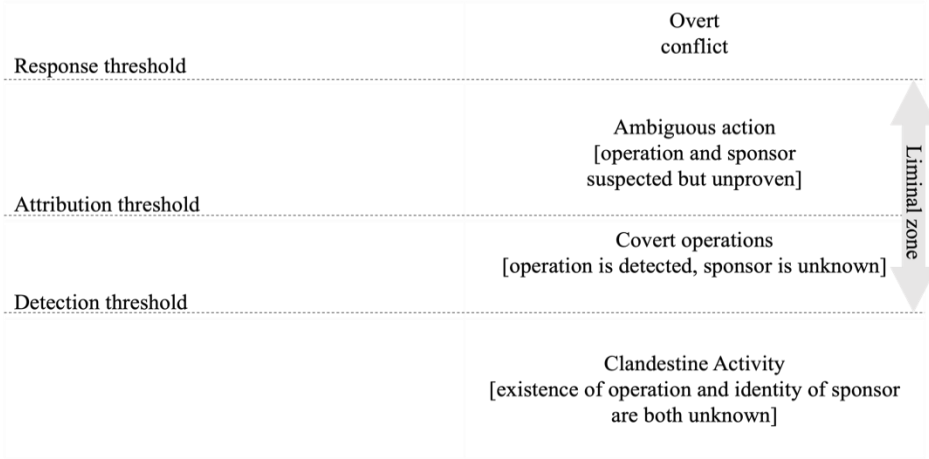

Figure 1. Liminal Warfare

Source: David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York, NY: Oxford University Press, 2020), 152.

The zone between detection and the adversary being able to fully attribute an action and respond is the ambiguous area where Russia excels.[90] This is a critical component of liminal warfare when it comes to fighting western powers such as the United States that rely on consensus building and international opinion, so they are constrained by the diplomatic thresholds of their political decision-makers before crossing the response threshold.[91] Understanding an enemy's political limits is paramount to liminal warfare

[90] Kilcullen, *The Dragons and the Snakes,* 153.

[91] Ibid.

and defines a space to operate below the response threshold.[92] There are five components to understanding what makes the adversary react and ways to extend or disrupt that threshold which is illustrated in figure 2.

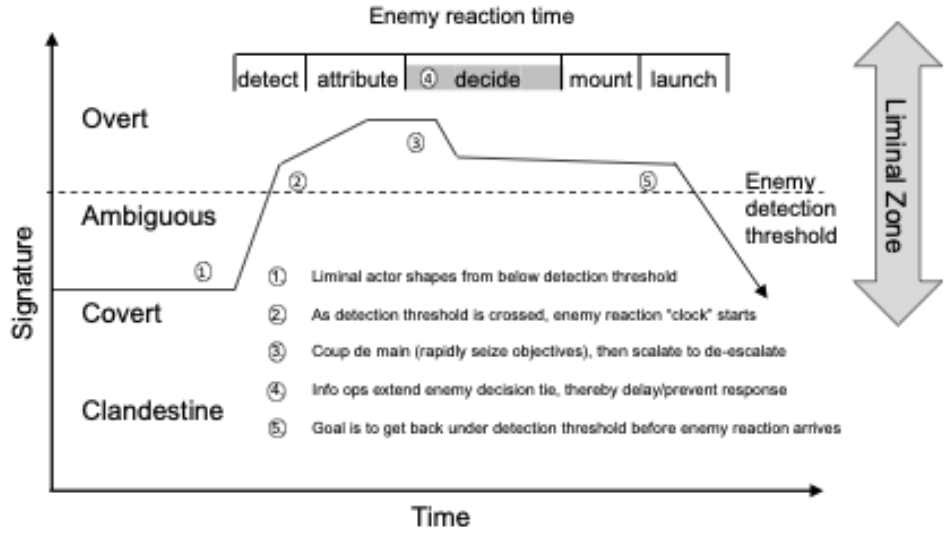

Figure 2. Sequence of a Liminal Warfare Operation

Source: David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York, NY: Oxford University Press, 2020), 158.

While not officially a Russian term, Russia utilizes the principles of liminal warfare in the information domain through a concept called *reflexive control*. This is where Russia seeks to cause "targets to act in the interests of the propagandist without realizing they have done so."[93] Russia's aim is to not just influence an audience on a certain topic as with traditional propaganda, but to influence their entire mental

[92] Kilcullen, *The Dragons and the Snakes*, 154.

[93] Ibid., 156.

framework, distorting their decision-making process, as described by S. A. Komov when he described the components of reflexive control as "distraction, overload, paralysis, exhaustion, deception, division, pacification, deterrence, provocation, suggestion, and pressure, all with the intent of manipulation."[94] Reflexive control is effective in that it is able to stay below the threshold of detection and comes from a place of ambiguity to cause people to act in Russia's interest without even realizing it.

Russia leverages these principles for its military to create relative advantages in the information environment. Looking at the role of the Russian military, it has four functions:

> 1. Deterring the military and political threats to the security or interests of the Russian Federation.
>
> 2. Supporting economic and political interests of the Russian Federation.
>
> 3. Mounting other-than-war enforcement operations.
>
> 4. Using military force.[95]

Intertwined into all these functions is information warfare, which is aimed at undermining the willingness of the opponent to fight and leveraging economic and political elements to shape the environment in countries of interest.[96] Russia is aggressive in the information domain to mask any deficiencies in the rest of its military, figure 3 shows Russia's Information Warfare concepts and principles they utilize.

---

[94] Kilcullen, *The Dragons and the Snakes*, 156.

[95] Ministry of Defence of the Russian Federation, "Mission and Objectives of the Russian Armed Forces," accessed January 6, 2022, https://eng.mil.ru/en/mission/tasks.htm.

[96] Paul et al., *A Guide to Extreme Competition with China*, 159.

Concept	Definition	Example	Domestic/Foreign/ Hybrid Use
Active measures	Using false or intentionally misinterpreted information to undermine the opponent's legitimacy or military power; using various forms of political repression to silence critics.	Forging letters about the implications of Sweden's future membership in NATO.	Hybrid
Deception (*maskirovka*)	A complex set of actions meant to deceive the enemy and hide true intentions through surprise, camouflage, deception maneuvers, concealment, use of decoys and dummies, or disinformation.	The appearance of "little green men" in Ukraine despite Russian denials of military involvement in the country.	Foreign
Reflexive control	"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."[a]	Disseminating information about alleged fascists in Ukraine and would-be benefits for citizens of eastern Ukraine if it became part of Russia.	Hybrid
Propaganda (black, gray, and white)	The use of information in a selective (white), partly true (gray), or outright wrong (black) manner that aims to convince the recipient to take or fail to take certain actions.	Information strategy employed by state-sponsored Russian media at home and abroad when reporting on Russian international engagements.	Hybrid
Censorship	Limiting freedom of expression under certain conditions, enforced either actively (e.g., through physical interruptions to digital connectivity) or through indirect influence (e.g., leading to self-censorship).	Active Russian control of domestic media and the Internet and preventing opposition figures from developing a large following.	Domestic
Intimidation	Influencing individual choices by implicitly threatening retaliation for undesirable choices or using nonlethal force, sham court trials, and other tools to indicate which behaviors are at odds with the interests of the intimidator.	Intrusions into the apartments of foreign journalists based in Moscow.	Domestic

Figure 3. Russian Information Warfare Concepts and Principles

Source: Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future US Army Operations in and Through the Information Environment* (Santa Monica, CA: Rand Corporation, 2018), 161.

Russia has invested heavily in its information warfare capabilities. These investments aim to provide capabilities to create an information advantage and provide its forces a broad framework when conducting operations in the information environment:

1. Control over the media to message both foreign and internal audiences.
2. Utilize social networks as a force multiplier.
3. Engage foreign audiences in their native language, relying on well-resourced proxies.
4. Develop an advanced EW capability.
5. Combine civilian and military capabilities to subvert opponents' defensive measures.[97]

Russia is continuing to invest in cyber technology including AI and ML to create an advantage in the cyberspace domain and thereby an informational advantage to support operational outcomes. Through this, Russia can spread disinformation and misinformation from multiple angles that pit their target audiences against each other and causes distrust in what is reported, which gives Russia an information advantage.[98]

In summary, Russia has long faced threats to its sovereignty from Western powers and has relied on information warfare to counter those threats. Russia's doctrine and

---

[97] Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future US Army Operations in and Through the Information Environment* (Santa Monica, CA: Rand Corporation, 2018), 152.

[98] Keir Giles, *Handbook of Russian Information Warfare,* Fellowship Monograph 9 (Rome: Research Division, NATO Defense College, November 2016), 51, https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf.

application of it have led to a long history of disinformation as a weapon to create a relative advantage over its adversaries by creating ambiguity to skirt around international laws and norms. Russia continues to invest in technology and capabilities to modernize and further perpetuate its information warfare tactics against strategic competitors.

US Information Advantage

Information warfare burst onto the scene for the US in the Gulf war, and the Army developed a FM specifically for Information Operations in 1996, however, most did not know how to leverage the effects of information collectively, so it eventually lost importance.[99] Many of the capabilities, such as electronic warfare, psychological operations, and ISR assets continued to work in support of kinetic effects, but they did so separately.[100] However, Libicki argues that "given today's circumstances, in contrast to those that existed when information warfare was first mooted, the various elements of information warfare should now increasingly be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations."[101]

Within the US military, information is used as an instrument of strategic power, plays into command and control, and intelligence collection.[102] From a strategic power

---

[99] Martin Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* 11, no. 1 (Spring 2017): 49, https://www-jstor-org.jsou.idm.oclc.org/stable/26271590?seq=1.

[100] Ibid., 50.

[101] Ibid.

[102] Eric X. Schaner, "MCDP 8, Information: A New Marine Corps Doctrine for the information Warfighting Function," *Marine Corps Gazette*, April 2022, 20, https://mca-marines.org/wp-content/uploads/MCDP-8-Information.pdf.

perspective, the US military has always said that it values information and it is one of the four instruments of national power but does little to incentivize commanders to take it into consideration when planning operations.[103] However, just as commanders would never go to battle without intelligence assets, they should view information in the same light. Information is vital to enhance decision-making and leveraging information gives the commander a relevant advantage over their adversary.

Information and leveraging it for advantage have become a top priority for US military senior leaders, as the 2018 National Defense Strategy points out "Information and the systems that gather, transmit, store, and process it has become the single biggest vulnerability in putative conflicts with China or Russia."[104] Information, in this military context, has three interrelated trends:

1. Military, information technology has become vital to the US maintaining an advantage over its adversaries.

2. Many new US systems that were strengths in the war on terror are vulnerable to strategic adversaries.

3. Strategic competitors China and Russia have prioritized creating an advantage over the US in any conflict by making the first move and degrading US information technology systems.[105]

---

[103] Schaner, "MCDP 8, Information," 21.

[104] Chris Dougherty, "Confronting Chaos: A New Concept for Information Advantage," *War on the Rocks*, September 21, 2021, https://warontherocks.com/2021/09/confronting-chaos-a-new-concept-for-information-advantage/.

[105] Ibid.

Chris Dougherty, who helped to shape the 2018 NDS shift in focus towards strategic competition, especially in the information space recently wrote, "Information advantage should be understood as gaining a temporary and contested edge in using information through technical systems, cognitive processes, and perceptual/psychological influence to achieve tactical, operational, or strategic advantages against a competitor in peacetime or an adversary in war."[106]

Most of US doctrine and military principles are geared toward conflict, as it is the job of the US military to fight and win the nation's wars. However, there is minimal guidance on how to compete with and create advantages over strategic adversaries along the competition continuum, especially in the information domain. However, Information Advantage is an emerging new term being introduced into Army doctrine, to include talking about relative advantage in the next FM 3-0 and completely rewriting ADP 3-13 to further define and expound upon this new term.[107] The current working definition for information advantage is "a condition when a force holds the initiative in terms of relevant actor behavior, situational understanding, and decision making through the use of all military capabilities."[108] There are five lines of effort that will be used to create an information advantage for the US:

[106] Dougherty, "Confronting Chaos."

[107] Mark Pomerleau, "Army to Set in Stone the Importance of Information Advantage, with New Capabilities On Deck," *C4ISRNeT*, July 01, 2021, https://www.c4isrnet.com/information-warfare/2021/07/01/army-to-set-in-stone-the-importance-of-information-advantage-with-new-capabilities-on-deck/.

[108] Hammerstrom, "Delivering the Information Advantage," 3.

1. Enable Decision Making: Enhance understanding of human and information dimensions; assure systems and processes for decision making.

2. Protect Friendly Information: Identity, secure, obscure, and defend friendly information systems from compromise or attack.

3. Inform domestic and international audiences: Provide timely factual information about US, Joint, Army, and combined operations to domestic audiences.

4. Influence foreign audiences: Assure allied, partner, and neutral audiences; and influence non-domestic perceptions and behaviors.

5. Conduct Information warfare: Attack adversary elements of combat power and defend friendly use of information against adversary information attack capabilities.[109]

This has been a topic of discussion over the past several years on what and how this new term "information advantage" should be defined, who should own it, and what it means for the military force. The cyber community has been a large proponent for information warfare, in fact, the Commander of Army Cyber Command, LTG Fogarty recently said, "The intent is to provide a proposal that will change us from Army Cyber Command to Army Information Warfare Command because we believe that is a more accurate descriptor of what I'm being asked to do on a daily basis."[110]

In 2018, *Department of Defense Strategy for Operations in the Information Environment* and the *Joint Concept for Operating in the Information Environment (JCOIE)* announced that Information would become a joint function, another sign that

[109] Hammerstrom, "Delivering the Information Advantage," 3.

[110] Mark Pomerleau, Pomerleau, Mark. "A New Name-and Focus-for Army Cyber Command?" *C4ISRNet,* August 21, 2019, https://www.c4isrnet.com/show-reporter/technet-augusta/2019/08/21/a-new-name-and-focus-for-army-cyber-command/.

senior leaders are looking to prioritize information.[111] However, this only identified gaps in the capabilities of the joint force and showed a need for entities such as special operations to evolve and prioritize improvements to meet this need.[112] The US special operations forces (SOF) community has always been a value proposition for the US as it was designed to shape the environment and create effects below the level of armed conflict.[113] As SOF provides a persistent presence worldwide and operates in this gray zone below open conflict, they act as a psychological deterrent for potential adversarial actors and can impose costs to adversary actions which can degrade their ability to conduct operations over time, which is an effective tool in competition.[114] This also allows for SOF to be sensors to collect information against strategic competitors that can be used to exploit their vulnerabilities or to mitigate any weaknesses by the US or its partners.[115] SOF are in a position to understand the needs of partner forces and are able to

[111] Christopher Paul and Michael Schwille, "The Evolution of Special Operations as a Model for Information Forces," *Joint Forces Quarterly* 100 (1st Quarter 2021): 9, https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=2&sid=bc1698ca-8615-49c1-940d-bd845193df09%40redis.

[112] Paul and Schwille, "The Evolution of Special Operations as a Model for Information Forces," 9.

[113] Isaiah Wilson III, "Rediscovering the Value of Special Operations," *Joint Forces Quarterly* 105 (2nd Quarter 2022): 38, https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=1&sid=170133a6-62a6-43fa-9216-56ce41bed49d%40redis.

[114] Hal Brands and Tim Nichols, "Special Operations Forces and Great-Power Competition in the 21st Century," (American Enterprise Institute, Washington, DC, August 04, 2020, 8, https://www.aei.org/research-products/report/special-operations-forces-and-great-power-competition-in-the-21st-century/.

[115] Ibid., 2.

train and equip local partners which give them confidence and make them less susceptible to the adversary's attempts to influence.[116] As SOF works in the competition continuum, it must also work to counter information disseminated by the adversary to exploit the vulnerabilities of US partners which may lead to an escalation of actions not favorable to US interests.[117]

ARSOF has the capabilities and a history of enabling information operations against lesser threats, but it now must adapt to facing strategic competitors with similar capabilities and a strategic focus on creating an information advantage for itself.[118] All three ARSOF elements (SF, PSYOP, CA) are tasked with collecting information to enable decision-makers to conduct follow-on operations. However, Psychological Operations (PSYOP) is the only organization within ARSOF that is trained to influence the behavior of foreign audiences which involves the science of understanding the target audience's susceptibilities and the art of how to deliver that message effectively.[119]

As the US shifts its focus from the global war on terrorism (GWOT) to competition with strategic competitors, it has left the Army special operations community

---

[116] James E. Hayes III, "Beyond the Gray Zone: Special Operations in Multidomain Battle," *Joint Force Quarterly* 91 (4th Quarter 2018): 64, https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/ pdfviewer?vid=1&sid=4d70a56a-2db7-4ee3-9428-8df177fe8532%40redis.

[117] Ibid., 65.

[118] Wilson, "Rediscovering the Value of Special Operations," 42.

[119] Mark Pelaez, "Hearts and Minds as Targets: PSYOP ANCOC Trains Inside the Box, but Thinks Outside of It, Too," *Special Warfare* 22, no. 4 (July 2009): 22-24, https://search-ebscohost-com.jsou.idm.oclc.org/login.aspx?direct=true&db=tsh&AN=44061376&site=eds-live.

in an identity crisis and needs to revamp how they operate to stay relevant.[120] For ARSOF to stay relevant in the competition continuum, it must understand its role to enable decision-makers, including those in other organizations. ARSOF will not be the lead effort as it was in the GWOT, so it will find that it will be in a supporting role and understand it must evolve to meet the new demands and continue to be a value proposition for the Army. In 2019, the US Army Special Operations Command (USASOC) Commanding General, Lieutenant General Fran Beaudette, acknowledged "To shake off the strategic atrophy" ... "we must evolve."[121] He directs the force to "shift the mindset and bring about evolutionary change"[122] As the competition watches and adapts its approach to counter the influence of the US, ARSOF must find ways to contribute in a new strategic environment of competition with China and Russia before the window of opportunity closes.[123]

---

[120] Brands and Nichols, "Special Operations Forces and Great-Power Competition in the 21st Century," 2; Edward Croot, "There is an Identity Crisis in Special Forces:Who are the Green Berets Supposed to Be?" (Fellows Strategy Research Project, U.S. Army War College, January 03, 2020), 1, https://sites.duke.edu/tcths_fellows/files/2020/04/Ed-Croot-Final-Paper.pdf.

[121] United States Army Special Operations Command (USASOC), *Army Special Operations Forces Strategy* (Fort Bragg, NC: USASOC, October 2019), 1, https://www.soc.mil/AssortedPages/ARSOF_Strategy.pdf.

[122] Ibid., 2.

[123] Joe Miller, Monte Erfourth, Jeremiah Monk, and Ryan Oliver, "Harnessing David and Goliath: Orthodoxy, Asymmetry, and Competition," *Small Wars Journal,* February 07, 2019, 3-6, https://smallwarsjournal.com/jrnl/art/harnessing-david-and-goliath-orthodoxy-asymmetry-and-competition; Brands and Nichols, "Special Operations Forces and Great-Power Competition in the 21st Century."

Summary

This review provided an overview of information and how it plays a role in warfare. It looked at strategic competitors China and Russia and how they view information, and information warfare specifically. Next it looked at information advantage and how it is a growing concern and driving policy for the US today. Finally, it explored the special operations community, and its role in competition in general and information specifically. The reader should come away with a better understanding of how China and Russia prioritize creating an information advantage across all efforts, both within the military and across their government. This is compared to the US and the military's view of information and how it has not been prioritized until recently. The US military is working to fix that by creating more emphasis through updates to doctrine and national policies. However, you should see a gap in that ARSOF has been designed to shape the environment and create effects below the level of armed conflict for the US Army, but ARSOF is unsure how to switch from its focus on the GWOT to strategic competition and contribute to the US gaining and exploiting an information advantage against China and Russia.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This chapter discusses the methods this thesis uses to answer the research question. This study uses a comparative case study to examine China and Russia's ability to create information advantage. It analyzes one case from Russia and one from China in which these countries attempted to use information to achieve national objectives. These analyses are used to produce an overall information advantage assessment for both China and Russia that describes and compares the information advantage strengths and weaknesses of each nation. Finally, these strengths and weaknesses are compared against ARSOF capabilities to determine where and how ARSOF can contribute to US information advantage by offsetting competitors' strengths and exploiting their weaknesses.

Comparative Case Study

A comparative case study is a method for analyzing historical data to make sense of current and real-world complex issues.[124] This method entails making a structured, focused comparison of the cases being studied. The structure comes from standardizing

[124] Zaidah Zainal, "Case Study as a Research Method," *Jurnal Kemanusiaan*, 5, no. 1 (June 2007): 1, http://psyking.net/htmlobj-3837/case_study_as_a_research_method.pdf.

data collection and measurement across cases. The focus comes from analyzing only certain aspects of the case that are related to the purpose of the study.[125]

A basic framework was used to structure the research to answer the primary and secondary research questions for this thesis.[126] The dependent variables are used in each case study to standardize the data to induce an aggregated assessment of each country's ability to gain information advantage. The focus comes from only looking at aspects of the case study that are relevant to actions taken that gained or inhibited information advantage.[127] This method was used to offset the limitations placed on the study of time and resources to conduct the research while giving it validity by utilizing reliable sources of data as a starting point for the analysis to make recommendations for the ARSOF community and further areas of study.

Case Selection Criteria

Three criteria were used to select the cases: strategic relevancy, information relevancy, and recency. Strategic relevancy means the case must examine China or Russia since these countries are the main strategic competitors to the US.[128] Information relevancy means that the case must involve China or Russia using information to achieve

[125] Alexander George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge: MIT Press, 2005), 67-72.

[126] Ibid., 67-68.

[127] Ibid., 70-72.

[128] U.S. President, *Interim National Security Strategic Guidance* (Washington, DC: The White House. March 2021), 8, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

national objectives. Finally, recency means the case occurs within the last 25 years. Recent cases are more likely to reflect future Chinese and Russian operations in the information space.

After evaluating several cases using the above criteria, two were selected for this analysis. The China case is about Chinese government actions in Africa from 2000 to 2020. The Russia case is about Russian operations in Ukraine from 2013 to 2014.

Case Analysis

The unit of analysis is information advantage-related actions in the Diplomatic, Information, Military, or Economic (DIME) domains. Each information-related DIME action is coded according to the information advantage line of effort (LOE) it supports. If an action supports more than one LOE, the action is coded separately for each LOE

Coded information-related DIME actions are then assessed using a three-level measure: successful (1), neutral (0), or backfire (-1). Successful (1) means the action contributed to China or Russia's information advantage. Neutral (0) means the action did not contribute to information advantage but also did not degrade it or contribute to an adversary's information advantage. Backfire (-1) means the action degraded China or Russia's information advantage or contributed to their adversary's information advantage. Table 1 shows an example of the coding and measurement framework:

Table 1. Independent Variable to Dependent Variable

#	Action	IA LOE	Assessment	Notes
R_1	Russia propaganda	3	1	
R_{2a}	Russia cyber ops	4	-1	
R_{2b}	Russia cyber ops	5	0	

Source: Created by the author.

Once all information-related DIME actions have been coded and measured, the next step is to produce information advantage LOE assessments for each case. The DIME actions in each LOE are assessed in aggregate to determine if each LOE is a strength or weakness for China. This process is repeated for Russia. All DIME actions are weighted equally towards the overall assessment.

The final step is a cross-case comparison of the LOE assessments. The Chinese and Russian assessments are compared to understand the similarities and differences between the two competitors. This comparison will inform the recommendations in the final chapter that discuss where ARSOF can contribute to US information advantage by offsetting competitors' strengths and exploiting their weaknesses.

Ethical Considerations

This study did not conduct any research through surveys or other means that involve human interactions. So, the researcher's primary ethical considerations for this research were ensuring that every source is cited correctly to give the author proper credit for their work and to differentiate their work from the author of this thesis. Also, the author worked to ensure that all case study data was analyzed was directly related to the framework of this research, that all relevant data was considered to ensure proper

assessments were made from the research and not taken from any predispositions on the topic from the author.

Summary

In the interest of time and brevity, the researcher chose to utilize a structured, focused case study comparison methodology to gather the data for this research to draw its analysis. This allowed the author to utilize real-world data to analyze and provide recommendations for future utilization and areas of further study. The topic of information advantage is an emerging term in the US Army, but many of the concepts have been in practice since the inception of warfare. This is a complex problem set, often taking years to determine causality vs. correlation of effects from actions taken in the information space. Utilizing case studies and comparing them gave ample data to induct conclusions and recommendations on ways and means that ARSOF can create and sustain an advantage over strategic competitors in the information domain.

CHAPTER 4

ANALYSIS

Introduction

This chapter will analyze the selected case studies of China focusing on its actions in Africa from 2000 to 2020 and Russia's actions involving Ukraine from 2013 to 2014. These case studies will help identify key strengths and weaknesses of each country's ability to create an information advantage, then will compare the findings for China and Russia's ability to create an information advantage for ARSOF to capitalize on opportunities moving forward in competition with these two countries.

China Case Study (Africa 2000-2020)

Strategic Context

China has had a relationship with many African countries since the 1960s. However, it was in 2000 when China began to formalize many of its partnerships with African countries through the creation of the Forum on China-Africa Cooperation (FOCAC) and Chinese investment in Africa dramatically increased.[129] Chinese assistance went from .08% of total assistance to 13% from 2002 to 2005 alone.[130] This increased

[129] Larry Hanauer and Lyle Morris, *Chinese Engagement in Africa: Drivers, Reactions, and Implications for US Policy* (Santa Monica, CA: Rand Corporation, 2014), 20, https://www.rand.org/pubs/research_reports/RR521.html.

[130] J. Stephen Morrison, Jennifer Cooke, Indira Campos, Michael Chege, Pat Utomi, and Alex Vines, *U.S. and Chinese Engagement in Africa: Prospects for Improving U.S.-China-Africa Cooperation* (Washington, DC: Center for Strategic & International Studies, July 2008), 2, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/080711_cooke_us_chineseengagement_web.pdf.

even more when China kicked off its global Belt Road Initiative (BRI) in 2013.[131] This initiative has spread Chinese economic and political influence worldwide; this is especially true in Africa, where they have BRI agreements with forty-one countries.[132] China has had a successful two-way relationship with many African countries, as China is in search of oil, gas, minerals, and other natural resources while also selling cheaply made Chinese goods and providing these countries with much need infrastructure upgrades.[133]

Often, to the benefit of pariah regimes, China does not require any preconditions or transparency from a government when it comes to having financial dealings, as is the case with the United States and its allies.[134] Another quiet, but significant development with the Chinese in Africa is the increase in military cooperation in the form of equipment sales and Chinese military presence and activities. China is not hesitant to sell to pariah governments, China sees much of the strife as a way to profit, as evidenced going from a 6% share in arms sales to top arms seller in Africa with a 25% share in 2010 as compared to only 3% for the US.[135] Chinese military involvement was initially limited

---

[131] R. S. Kalha, "An Assessment of the Chinese Dream: 2015," *Strategic Analysis* 39, no. 3 (2015): 274, https://www.tandfonline.com/doi/full/10.1080/09700161.2015.1022317.

[132] Steven Feldstein, *Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa* (Washington, DC, May 8, 2020), 2, https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.

[133] Hanauer and Morris, *Chinese Engagement in Africa*, 27.

[134] Ibid.

[135] Ibid., 39.

to weapons sales and unilateral UN peacekeeping missions,[136] however, that all changed with the opening of the first PLA overseas base and conducting joint exercises in Djibouti in 2017.[137]

China is very concerned about how they are perceived internationally, and Africa is no exception. There has been an increased emphasis within China to educate their own citizens on Africa to better its relations with Africa. Also, China has incentivized its journalists to go and work in Africa to inform Africans about the benefits of working with China and to dispute western media reports that could potentially damage African perceptions of China.

Overall, China has been very successful in establishing relationships with African nations through diplomatic and economic influence. This has allowed China to wield influence over these countries in settings like the UN. This influence has also gained China the access to build much of Africa's digital infrastructure giving them the ability to exploit it, leading to an information advantage over all other competitors in that space.

Case Study Findings

Table 2 is a summary of the results that were recorded for this research, with the full list of results located in appendix A.

---

[136] Hanauer and Morris, *Chinese Engagement in Africa,* 115.

[137] Zach Vertin, *Great Power Rivalry in the Red Sea: China's Experiment in Djibouti and Implications for the United States* (Washington, DC: The Brookings Institution, June 2020), 1, https://www.brookings.edu/wp-content/uploads/2020/06/FP_20200615_china_djibouti_vertin.pdf.

Table 2. Summary of Chinese Case Study Results

	LOE Coding Results			
	Successful	**Neutral**	**Backfire**	**Total LOE**
1. Enable decision makers	5	2	1	8
2. Protect friendly information	0	3	0	3
3. Inform domestic and foreign audiences	3	3	3	9
4. Influence foreign audiences	17	6	7	30
5. Conduct information warfare	3	6	0	9
Total Actions	28	20	11	59

Source: Created by the author to summarize the results of the research.

LOE 1: Enable Decision Makers

The analysis showed this LOE to be a strength for the Chinese as five of the eight results were coded as successful in enabling Chinese decision-makers. The results in this study coded to this LOE were actions taken to put China in a positive light. China used its status as a key trade partner and standing within the UN to ease tensions between African countries. A second observation was the increase in military presence on UN peacekeeping missions which went from strictly unilateral missions to increasing its joint training exercises with African partners, which successfully allows China to have more input into conflict resolution. China also went against its own policies by opening its first PLA overseas base in Djibouti just miles from a long-established US base. China has evolved over time in how it views its role in Africa, which has opened countless opportunities for China to operationalize its military in support and enable its decision-makers to achieve its objectives for the region.

LOE 2: Protect Friendly Information

The analysis showed this LOE to be neutral for the Chinese as all three results were coded as neutral in protecting friendly information. As the case study is not based in conflict, it is impossible to fully understand China's ability to protect its information from this case study. However, the small sample size showed that China will go to great lengths to protect information that it deems important. This is evidenced by China demanding restricted air space over its military base in Djibouti as they were fearful of the US flying ISR assets over its base and uncovering whatever secrets they may have on its base. A second example is China working to impede UN investigations into China's sale of weapons that end up in the hands of rebel groups. China has been reported as being willing to sell weapons to any government and turns a blind eye to who ends up with those weapons, which is something they wish to hide. A final example may show that they are vulnerable, but they continue to support governments in Africa that suppress any public dissent towards the government, especially any dissent directed at China.

LOE 3: Inform Domestic and Foreign Audiences

The analysis showed this LOE to have been equally split across all nine coded results actions that were successful, neutral, and backfired for informing domestic and foreign audiences. While it would not be considered a strength by this metric, China has recognized its shortcomings and is working to rectify them. China has made a push to increase its ability to inform Africans through an increased news media presence in Africa, as evidenced by China spending $6.6 billion dollars in 2009 for this expansion which expanded Chinese TV, newspaper, and radio on the continent. This was done to

directly refute western media reporting on China as they believed it was harming Sino-African relations and advancing its policy goals in Africa.[138]

In 2013, seeking to better their relationship and engender the goodwill of Africa, China increased its cultural exchanges and initiatives, allowing for African students, political, military, and business leaders to travel to China, giving many of them an opportunity of a lifetime while giving them free training and instructing them on the Chinese way of conducting business.[139] China has emphasized showing Africa that it prioritizes its relationship, as Africa was the first overseas trip for the past two Chinese presidents and many of its senior officials. A large reason for this push, is to increase the public image and perception of China in Africa due to pockets of unrest among Africans who feel that China has come and taken away their jobs and flooded the African market with cheaply made Chinese goods.

LOE 4: Influence Foreign Audiences

The analysis showed this LOE to be a strength for the Chinese as seventeen of the thirty coded results showed the Chinese influencing Africans successfully. Results coded under the influence LOE accounted for half of the fifty-nine findings, making it the most important aspect and most used and effective tool for Chinese actions in Africa. China wields its influence through a myriad of ways to include BRI and developmental aid programs, the Chinese can leverage many African countries' economic dependence upon China to influence them politically. As exemplified by Malawi receiving a large infusion

[138] Hanauer and Morris, *Chinese Engagement in Africa,* 97.

[139] Ibid., 99.

of Chinese financial investment when it recognized Beijing and its One China policy and cut diplomatic ties with Taiwan in 2008.[140]

African leaders seek to be respected on the global stage, and China goes out of its way to treat them as leaders of sovereign states and as equals, making sure to point out the differences in how China treats them as compared to Western powers and how they continue to treat them.[141] China emphasizes the perception that they are in Africa to support Africa, while western countries are there to get rich from their natural resources. For example, the Chinese point out the extravagant style of living for western workers compared to Chinese workers who live frugally, thus spending 95 cents on the dollar towards projects benefiting Africans as compared to the western agencies who spend 80% on their own staff.[142] On the negative side, while it is not currently manifesting itself, the high ratios of debt that China leverages for influence could end up hurting their relationships with many of these African countries, if those countries are unable to pay back these loans, and there are numerous reports of Chinese-built infrastructure failing long before it should.[143]

LOE 5: Conduct Information Warfare

The analysis showed this LOE to be neutral for the Chinese as six of the nine results were neither positive nor backfired. This does not mean that China does not have

---

[140] Hanauer and Morris, *Chinese Engagement in Africa,* 29.

[141] Ibid., 32.

[142] Ibid., 38.

[143] Ibid., 45.

the capability or appetite for this type of warfare, it only means they have not utilized it yet in Africa but are laying the groundwork to do so. For decades, China has financed and built over 70% Africa's digital infrastructure. As a part of this, China offers governments safe and smart city technology, which allows governments to utilize it as surveillance and online censorship tools, which reinforces many of these governments' propensity to repress any political opposition.[144] With China responsible for building much of Africa's digital infrastructure, China has access to all African networks and a treasure trove of data and information that it can exploit to maintain political leverage over African countries and create an economic dependence upon China.[145] China is also leveraging its access to the safe city facial recognition programs to enhance and diversify its data lake to expand its own artificial intelligence capabilities which can have unforeseen consequences.[146]

China Case Study Summary

The findings from this case study showed that China successfully executed lines of effort for enabling its decision makers and influencing its intended audiences in Africa. While the other three lines of effort had largely neutral results, this does not mean that

---

[144] Hanauer and Morris, *Chinese Engagement in Africa*, 2.

[145] Lingling Wei, "China's New Power Play: More Control of Tech Companies' Troves of Data," *The Wall Street Journal*, June 12, 2021, https://www.wsj.com/articles/chinas-new-power-play-more-control-of-tech-companies-troves-of-data-11623470478.

[146] Samuel Woodhams, "How China Exports Repression to Africa: China's "techno-dystopian expansionism" is undermining democracy in African countries," *The Diplomat*, February 23, 2019, https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/.

China does not prioritize those lines of effort. There is evidence that China has put a strong emphasis into improving the inform line of effort through an increased media presence in Africa. Results for the protect friendly information and conduct information warfare lines of effort were sparse for this case study, however, this only means they have not actioned these lines of effort yet, but they have laid the groundwork to be more active on both fronts. As mentioned in the literature review, China goes beyond social norms and finds ways to bend the rules and shape the environment in unconventional ways.

Russia Case Study (Crimea 2014)

> The most amazing information warfare blitzkrieg we have ever seen in the history of information warfare.
>
> —GEN Phillip Breedlove, USAF, Supreme Allied Commander Europe (2013-2016), quoted in Peter Pomerantsev, "Russia and the Menace of Unreality"

Strategic Context

The essence of the Russian invasion of Crimea in 2014 came down to Russia feeling the need to protect its security interests from western influence spreading closer to their border and tip the balance of power in the Black Sea region to Russia. Losing control of this region would result in Russia losing its ability to be a true Eurasian empire.[147]This was brought to a head as Ukraine was looking to join the European Union

[147] Stephen Larrabee, Peter Wilson, and John Gordon, *The Ukrainian Crisis and European Security: Implications for the United States and the US Army* (Santa Monica, CA: Rand Corporation, 2015), vii, https://www.rand.org/pubs/research_reports/RR903.html.

(EU) and the NATO alliance, which would severely limit the influence Russia would be able to exert over Ukraine and lose a buffer zone between Russia and NATO countries.

In the end, Russia was able to take advantage of and exploit political unrest in Ukraine that turned violent to mass troops on the border for security purposes and create a cloud of ambiguity over its objectives which created time and space for Russia to act.[148] Russia learned from its past mistakes from its dealings with Georgia in 2008 which was armed with NATO equipment and implemented hybrid warfare tactics to exploit Ukrainian weaknesses while staying below the detection threshold leading up to and through the infiltration of Ukraine in 2014. Russia utilized disinformation as the primary tool for obfuscating its true intentions and creating division among European countries, which gave Russia time and space to operate and achieve their objectives.[149]

Russia showed an incredible ability to leverage the concepts of reflexive control and hybrid warfare through its disinformation and cyber campaigns. However, some of the short-term victories they achieved in Crimea, may be at the expense of their long-term success. Unless Russia develops lessons learned and changes how they operate, many of their standard operating procedures have been exposed and are less likely to work again.[150]

---

[148] Larrabee, Wilson, and Gordon, *The Ukrainian Crisis and European Security*, viii.

[149] 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, https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

[150] Ibid., 21.

Case Study Findings

Table 3 is a summary of the results that were recorded for this research, with the complete list of results located in appendix B.

Table 3. Summary of Russian Case Study Results

	LOE Coding Results			
	Successful	**Neutral**	**Backfire**	**Total LOE**
1. Enable decision makers	9	1	0	10
2. Protect friendly information	1	3	0	4
3. Inform domestic and foreign audiences	0	3	0	3
4. Influence foreign audiences	6	7	1	14
5. Conduct information warfare	7	2	0	9
Total Actions	23	16	1	40

Source: Created by the author to summarize results of the research.

LOE 1: Enable Decision Makers

The analysis showed this LOE to be a strength for Russia as nine of the ten results were coded as having positive effects on enabling decision-makers. Russia did a masterful job at enabling its decision-makers to use information to gain an advantage by using disinformation. The Russians were able to create and add to the chaos of the Ukrainian political situation which bought Russia time and space to put its plan into play of massing troops at the border without raising any alarms from the international community. This resulted in Russia being able to take over Ukrainian military bases quickly and quietly in Crimea. The disinformation of Russia not being directly involved

with the invasion also allowed it to be a neutral third party in the peace talks which allowed Russia to maintain influence without taking any responsibility for preserving the peace.

LOE 2: Protect Friendly Information

The analysis showed this LOE to be neutral for Russia as three of the four results were coded as having neutral effects for protecting information. However, the lack of findings that backfired may prove this as a strength for Russia as many of its actions were undetectable. Russia used disinformation and proxy forces to protect information vital to the successful completion of its objectives. Russia also utilized non-state patriotic hackers to do their mission, which left enough doubt on whom they worked for or who hired them.[151]The ability to obfuscate the size of its force and its activity on the border and hide behind mercenary forces allowed Russia to hide its intentions from international powers and gave them the advantage of surprise in Ukraine. Although, with most of Russia's operations being built around deception, it will be hard for Russia to carry out this type of operation using the same tactics again.

LOE 3: Inform and Educate Foreign and Domestic Audiences

The analysis showed this LOE to be neutral for Russia as all three results were coded as having neutral effects for informing foreign and domestic audiences. The distinction between the LOEs inform and influence for Russia is murky at best, as Russia

[151] Glib Pakharenko, "Cyber Operations at Maidan: A First-Hand Account," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 67, https://ccdcoe.org/uploads/2018/10/Ch07_CyberWarinPerspective_Pakharenko.pdf.

uses its media platforms and diplomatic officials to spread propaganda and disinformation, which is assessed to be more geared towards influencing over informing. This is evidenced by Russian news outlets worldwide, being state-owned and could hardly be seen as a legitimate source to inform both domestic and foreign audiences.[152] All three results that were categorized as Russia informing both domestic and foreign audiences were later found to be disinformation campaigns that had little to no effect on audiences outside of the immediate influence of Russia.

LOE 4: Influence Foreign Audiences

The analysis showed this LOE to be a mix of successful and neutral for Russia as seven of the 14 results were coded as having neutral effects and six were coded as successful for influencing foreign audiences. Russia had three primary targets for its influence campaign, the first was NATO and other European powers, the second was the Ukrainian government, and the third was the civilian population both domestic and international. Russia's aim with its propaganda was not necessarily to change the narrative but to distort information for western audiences that would disrupt their ability to discern truth from disinformation and lose trust in its media and begin to create rifts and distrust between allies.[153] Russia also leveraged a substantial social media presence to create and spread this misinformation and disinformation. Before the invasion, the Russian propaganda arm incessantly messaged that the government of Ukraine was

[152] Natalka Pisnia, "Why Has RT Registered as a Foreign Agent with the US?" *BBC News*, November 15, 2017, https://www.bbc.com/news/world-us-canada-41991683.

[153] Snegovaya, *Putin's Information Warfare in Ukraine*, 14.

illegitimate, utilizing 'reflexive control' to influence both internal and foreign audiences to Russia's advantage.[154]

LOE 5: Conduct Information Warfare

The analysis showed this LOE to be a strength for Russia as seven of the nine results were coded as having successful effects for conducting information warfare. Before the conflict, Russia leveraged proxy hackers to conduct Distributed Denial-of-Service (DDoS) attacks to shut down Ukrainian political and economic websites and disrupted communications for Ukrainian officials which exploited the unrest in Ukraine.[155] Once the invasion occurred, Russia immediately moved to sever communication nodes for the Ukrainian Army while taking advantage of Russian-built, Ukrainian communications to continue to collect intelligence on Ukrainian operations.[156] For example, Russia utilized EW and Signals Intelligence (SIGINT) capabilities to collect on Ukrainian positions to call in artillery fire, destroying those units.[157]

Russia Case Study Summary

The findings from this case study showed that Russia was successful in enabling its decision-makers and conducting information warfare. Russia primarily relied on disinformation as a means of enabling its decision-makers and conducting information warfare. While the influence line of effort results was fairly split between successful and

[154] Snegovaya, *Putin's Information Warfare in Ukraine*, 12.

[155] Pakharenko, "Cyber Operations at Maidan," 59.

[156] Ibid., 62.

[157] Ibid., 63.

neutral, the fact that they were able to influence Western countries from truly intervening in the conflict would mean Russia was successful in influencing foreign audiences. The protect friendly information and inform lines of effort findings were neutral for Russia, but for very different reasons. In protecting friendly information, Russia was able to leverage ambiguity and deception to keep western powers guessing as to its true intentions in the Ukrainian conflict. With the inform line of effort, it is a bit of a misnomer to say that Russia tries to inform both domestic and foreign audiences, as all news outlets and diplomats are all working under the guidance of the state and could be considered influence actions. Russia's approach is limited in nature, as most disinformation has a shelf life and works best when there is already some sort of chaos ensuing or the adversary is not united in their response.[158] The Russian military is overly reliant on deception and disinformation to gain advantages and compensate for weaknesses in other areas which could lead to Russia's eventual demise as they continue to isolate themselves.[159]

China, Russia Comparison

While there is no direct correlation or interaction between China and Russia in either of these case studies, it does give a better sense for the strategic competition space and across the five lines of effort related to gaining an information advantage This will help to create recommendations for ARSOF to effectively contribute to an information advantage for the US that could affect both competitors.

---

[158] Snegovoya, *Putin's Information Warfare in Ukraine*, 18.

[159] Ibid., 10.

Table 4. Summary of China and Russia Case Study Findings

	China	Russia
1. Enable decision makers	Strength	Strength
2. Protect friendly information	Neutral	Neutral
3. Inform domestic and foreign audiences	Neutral	Neutral
4. Influence foreign audiences	Strength	Strength
5. Conduct information warfare	Neutral	Strength

Source: Created by the author to summarize case study findings.
NOTE: Findings in table 4 were derived from a quantitative measure of the coded results of whether the action was successful, neutral, or backfired across the five lines of effort for information advantage from tables 2 and 3. If the results were inconclusive, the author made a qualitive assessment to determine the finding.

Both China and Russia go about gaining and exploiting information advantage in different ways, but they prioritize and utilize the same lines of effort to accomplish their objectives. This is very interesting as these two case studies showed two countries in two very different situations, acting in very distinctive ways with different objectives. China continues to expand their BRI, digital silk road (DRS), and military presence which gives them influence and sensors worldwide to better utilize its OODA loop in the information environment. The Russians on the other hand utilize disinformation to create and exploit chaotic situations that give them time and space to accomplish its objectives.

There were few results in either case study on how either China or Russia protects their information, which is most likely due to the classification of this study. However, with the rollouts of safe and smart cities in Africa and beyond, it will become increasingly harder to protect US information from the Chinese when operating in those

areas. And Russians like to hide behind a wall of deception, this allows them to hide their true intentions as long as possible.

The idea of informing both domestic and foreign audiences is more of a western concept. Both countries have poured incredible amounts of resources into media outlets to combat western influence and refute western narratives. However, both countries' governments own these media outlets, causing them to be little more than puppets for their government and propaganda arms working to influence both domestic and foreign audiences rather than simply informing them.

Both China and Russia go about it very differently but are successful at influencing their intended audiences. China leverages its economic and diplomatic avenues to influence foreign governments to do their bidding. At the same time, Russia continues its tradition of disinformation and the concept of reflexive control to push people towards acting in a way that is beneficial to them. They both pose unique dilemmas for the US and how to counter their approaches to influence.

Looking at each case study, Russia had more opportunities to conduct information warfare as it was operating in a conflict zone with military power involved. Russia showed a propensity to leverage cyber, SIGINT, EW, and other technical means to gain advantages over the Ukraine government and NATO countries looking to intervene. China, on the other hand, had little reason to conduct information warfare in Africa. Still, one can easily see that they have laid the groundwork to conduct information warfare if it is deemed necessary as it has built and has access to a large majority of the digital infrastructure of Africa and anywhere it has developed safe and smart cities.

Overall Summary

Looking at the approach of both countries, it is easy to see that China has more of a long-term strategy to accomplish its objectives. China's rise to the global stage has been peaceful, but that just means that it is more of a challenge for the US to compete with. With the goal of being the predominant global power, China views information as a critical tool for accomplishing its international objectives without having to go to war in a traditional sense. They are deliberate in their approach and working to build a network of countries and governments beholding to them, which China can use for future leverage while extracting much-needed natural resources that it cannot organically produce. Russia, on the other hand, appears to have a much shorter vision as it employs disinformation as a critical weapon in its arsenal. Russia works through proxy forces and through means that are difficult to attribute directly back to them, allowing for plausible deniability. Russia acts in a manner that is hard to predict, making it hard to plan for at times, but also makes it susceptible to facing a unified front while becoming more isolated.

Of the two competitors, China is the pacing threat to the US. According to the undersecretary of defense for policy Colin Kahl, "It means that China is the only country that can pose a systemic challenge to the United States in the sense of challenging us, economically, technologically, politically and militarily."[160] While both countries are priorities for US policy decision-makers to compete against in the grey zone, Russia is

[160] Jim Garamone, "Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence," *DoD News*, June 2, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2641068/official-talks-dod-policy-role-in-chinese-pacing-threat-integrated-deterrence/.

seen as an actor that must be deterred, while China is clearly the number one priority moving forward.[161]

[161] Garamone, "Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence."

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> Whether it be the intrusions of hackers, a major explosion at the World Trade Center, or a bombing attack by bin Laden, all of these greatly exceed the frequency bandwidths understood by the American military...This is because they have never taken into consideration and have even refused to consider means that are contrary to tradition and to select measures of operation other than military means.
>
> —Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*

Introduction

This chapter examines the implications this study has for ARSOF and information advantage. It recommends three ways that ARSOF can contribute to US information advantage based on the case study findings. To better understand how to gain an information advantage over strategic competitors, ARSOF must be able to first understand what the competitor is capable of. The literature review and individual case studies show how strategic competitors China and Russia think about information and how they have leveraged it to gain an advantage. The case study analysis shows examples of how these countries operate and what ARSOF will face when deployed. ARSOF is in a unique position to contribute solutions and to take advantage of the opportunities it is presented to gain an information advantage over strategic competitors such as China and Russia.

ARSOF Capabilities

ARSOF is uniquely trained and organized, and many ARSOF capabilities have significant latent potential to contribute to competition against China and Russia in the

information space. ARSOF includes the Special Forces (SF) Regiment, Psychological Operations (PSYOP) Regiment, Civil Affairs (CA) Regiment, Ranger Regiment, and the Special Operations Aviation Regiment (SOAR). Each component brings special capabilities that contribute to the overall core competencies as shown in figure 4, but the recommendations will focus primarily on the SF, PSYOP, and CA forces.[162]

Regional PSYOP Teams (RPTs) are deployed worldwide and work closely with US embassies and partner nation allies to enhance their resiliency against threats to US interests to deny freedom of movement in the information environment. Civil Affairs (CA) teams are employed to develop infrastructure and promote the US as a key partner and establish civilian-military relationships, which if leveraged properly, are beneficial in the information domain. SF detachments primarily work by, with, and through host nations and other multi-national partners. SF is organized, manned, trained, and equipped to execute preparation of the environment tasks, unconventional warfare, foreign internal defense, and security force assistance with partner nations to make them more capable of resisting threats.[163]

[162] John F. Mulholland Jr., "Countering Irregular Threats the Army Special Operations Contribution," *Joint Force Quarterly* 56 (1st Quarter 2010): 71-75.

[163] Headquarters, Department of the Army, Field Manual 3-18, *Special Forces Operations* (Washington, DC: Army Publishing Directorate, 2014), chap. 2, https://armypubs.army.mil/epubs/DR_pubs/DR_c/pdf/web/fm3_18.pdf.

United States Code Title 10, Section 167 **Unified Combatant Command for Special Operations Forces**	***Department of Defense Directive 5100.01*** **Functions of the Department of Defense and its Major Components**	***Joint Publication 3-05*** **Special Operations**
• Civil Affairs • Counterterrorism • Direct action • Foreign internal defense • Humanitarian assistance • Military information support operations • Strategic reconnaissance • Such other activities as may be specified by the President or the Secretary of Defense • Theater search and rescue • Unconventional warfare	Subject to this authority, direction and control of the Secretary of Defense, Commander, U.S. Special Operations Command is responsible for and has the authority necessary to conduct, in addition to those specified, all affairs of such command relating to special operations activities, including— • Civil Affairs operations • Counterproliferation of weapons of mass destruction • Counterproliferation operations • Counterinsurgency • Direct action • Foreign internal defense • Information operations • Military information support operations • Security force assistance • Special reconnaissance • Unconventional warfare	• Civil Affairs operations • Countering weapons of mass destruction • Counterinsurgency • Counterterrorism • Direct action • Foreign humanitarian assistance • Foreign internal defense • Hostage rescue and recovery • Military information support operations • Preparation of the environment • Security force assistance • Special reconnaissance • Unconventional warfare

Figure 4. Special Operations Activities

Source: Headquarters, Department of the Army, Army Doctrine Publication 3-05, *Army Special Operations* (Washington, DC: Army Publishing Directorate, 2019), 1-07.

Recommendation #1: Prioritize Missions and Resources

The first recommendation is for ARSOF to understand where China and Russia are competing in the information space and prioritize ARSOF missions and resources to those spaces. This recommendation aims to mitigate China and Russia's influence and enable ARSOF decision making. The findings in Chapter 4 show that both China and Russia prioritize influencing audiences to gain an information advantage to achieve their objectives. And, both countries have had success in this line of operation.

To have an effective mission and resource priorities, commanders must be able to make informed decisions. They need access to relevant and reliable data for their areas of operation to find where ARSOF will be most value-added in the competition space. This will require ARSOF to gain a better understanding of where China and Russia are active, and what actions have been successful, had no impact, or backfired for China and Russia.

Another necessary step is to develop measurable objectives to show where partners and ARSOF are having effects. This will enable decision-makers to reinforce success and leverage their forces along all five lines of effort to exploit opportunities to gain an information advantage. Understanding whether activities are contributing successfully towards mission accomplishment (or not) will enable ARSOF to adjust its mission priorities more effectively. This will also help to create a better case for causation over correlation and provide continuity between deployment cycles, so the new teams on the ground do not have to start back at zero but will come armed with data that shows what worked and what didn't to shape operations moving forward.

Recommendation #2 Take a Holistic Approach to Information Advantage

The second recommendation is for ARSOF to take a holistic approach to information advantage that integrates all three ARSOF elements for maximum effects. China has shown the ability to exert influence through a multi-pronged approach across the DIME construct to influence local governments to accept that it has their best interest in mind, while also conducting message campaigns to discredit US efforts in the same area as self-serving. This recommendation will also work to exploit the findings that showed Chinese weakness in not assimilating with the local culture. Russia also seeks to influence through disinformation and creating division that can be exploited by its

decision-makers. Chinese and Russian actions do not fall neatly within a single ARSOF element's purview. As such, it is important that ARSOF synchronize the effects of all three elements in information competition with China and Russia.

ARSOF senior leaders should mandate that geographically aligned ARSOF elements work together. This would open the door to higher levels of collaboration during pre-mission planning, training, deployment, developing lessons learned, and providing continuity for follow-on teams. Each ARSOF element brings unique capabilities that jointly create greater effects in mitigating Chinese and Russian influence than if the three elements work separately.

This author's personal experience suggests ARSOF teams often deploy having never met with the teams from the other two elements or understanding what the others' mission is. This approach limits their ability to understand how they could collaborate in accomplishing mutually beneficial objectives, which would ultimately benefit the US by ARSOF providing a unified approach to information advantage. Presently, nothing forces teams to train or work together. As a result, opportunities to gain an information advantage may be missed. Forcing all three elements to understand each other's capabilities and work together would lead to maximizing information advantage effects that would counter Chinese efforts to influence through BRI and propaganda slandering US intentions, and Russian attempts to create and exploit the chaos.

Recommendation #3: Compete Aggressively

The final recommendation is for ARSOF to be more aggressive by mimicking some of the strengths of China and Russia and exploiting their weaknesses. China has demonstrated the willingness and ability to spread its influence by expanding its network

and nurturing relationships to maintain its influence as evidenced by its BRI deals in Africa. They do enough to placate the government and line their pockets with kickbacks while underpaying unskilled local laborers and causing many to lose their jobs. While the Russians also present a unique challenge, as they tend to operate through proxy forces and use ambiguous means to influence tenuous situations towards instability. These actions benefit Russia and enable its decision-makers to achieve its strategic objectives. However, Russia tends to be inflexible in deviating from its plan, and many of its technological advantages technologically can be offset as evidenced by Ukraine switching its security measures disrupting Russian EW and SIGINT capabilities.

Rather than allowing China and Russia to dictate the terms of competition, ARSOF must develop operations to sense, test, and probe Chinese and Russian decision-makers and put them on the defense. This will illuminate how Chinese and Russian decision-makers make decisions and how to degrade or disrupt their ability to exert influence in ARSOF areas of operation. Disrupting and degrading influence—which the findings in Chapter 4 suggest is a key line of effort for both nations—will significantly reduce Chinese and Russian information advantage. Other countries will lose trust in China's ability to complete their end of the deal, and lead to China having to spend more resources on projects than estimated. This will, in turn, lead to increased financial burden and extended timelines as they deal with the effects of ARSOF actions. Russia's disinformation campaigns can be a strength but can also be a weakness for them. Disinformation is only effective if believed. ARSOF can act as sensors to locate and preemptively debunk Russia's information campaigns. This will take the advantage of surprise away from the Russians and help to inoculate and unify partner nations against

their influence, which exploits Russia's weakness of not deviating from their plans and puts them on the defensive.

ARSOF should also mimic some aspects of Russia's reflexive control. ARSOF typically puts a US face on its operations to show that the US is a good partner and benefits the host nation. Taking a reflexive control approach, however, would involve inducing host nations to voluntarily take action advantageous to the US or disadvantageous to China or Russia. This approach will take longer to establish and execute but will have a greater impact as those impacted will believe they are deciding in the best interest of themselves. ARSOF may not necessarily need to influence nations closer to the US as long as they push support away from China and Russia, which in some ways is just as important and will create an information advantage for the US in that country.

A caveat to this recommendation is that these actions will occur outside a declared theater of armed conflict. They would require US State Department and perhaps Congressional approval. As such, political sensitivities are likely to limit operations against strategic competitors that could be considered provocations. Consequently, ARSOF will need to build relationships and trust with other government agencies, host-nation partners, and allies operating in the same region to ensure actions are aligned with US strategic and political goals.

Recommendations for Further Study

This research covered a large topic with a lot of strategic implications for ARSOF and the US when dealing with strategic competitors China and Russia. There are many

more topics of concern that would be recommended for future and further study as the scope and time for this study would simply not allow for them to be covered properly.

As the current Russian invasion within Ukraine happened towards the end of the research for this thesis, it was not feasible to incorporate the data from the past few months. However, this would be a very interesting topic of study in the future as more clarity is gained on the situation, especially as early indicators suggest Ukraine and other European countries are handling information advantage in this conflict much better than the 2014 conflict. It would be beneficial to compare this conflict against the other Russian incursions, namely Georgia in 2008 and Crimea in 2014, to glean out what the differences were and why the results were the way they were. This would help to see how Russia and other European countries have evolved over time, especially from an information advantage perspective.

While this research looked at China and Russia individually, it would be beneficial to look at them as a group. As Russia goes into isolation due to its actions in Ukraine, they may be pushed to work closer with China in a relationship of convenience. Both countries working together would have the potential to be detrimental to the US and its goals. However, it could also be something that could be exploited as the two countries have a tenuous relationship with previous border disputes and converging areas of interest such as the natural resources in the Arctic.[164]

[164] Paul Stronski and Nicole Ng, *Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic* (Washington, DC: The Carnegie Endowment for Interational Peace, February 28, 2018), https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and%20china-in-central-asia-russian-far-east-and-arctic-pub-75673.

From an ARSOF perspective, it would be good to look further into creating a proponent for creating an information advantage and understanding what that would look like. Or even look at if ARSOF should be the proponent for the entire SOCOM enterprise? As information advantage is an emerging concept for the Army, someone needs to be responsible for operationalizing this concept, or else it will turn into a good idea that many want, but few know how to incorporate.

Concluding Thoughts

The concept of ARSOF contributing to the US gaining and exploiting opportunities to gain information advantage over China and Russia is a broad topic that cannot be properly covered in one paper. This research shows that this is a complex environment, and ARSOF will need an iterative approach to probe and sense how these strategic competitors respond. As advantage is often fleeting, ARSOF must continue to gain awareness on how to exploit opportunities to gain an information advantage. In the end, ARSOF is just one component for the US to leverage in gaining an information advantage over China and Russia, so ARSOF must continue to evolve past the GWOT to operating along the competition continuum against China and Russia, to provide a value proposition to give the US an advantage moving forward.

APPENDIX A

CHAPTER 4 RESULTS (CHINA)

#	Action	IA LOE	Assessment	Notes
C1	China demand is quickly outpacing Africa's resources[165]	1	0	China's domestic use of resources such as oil is outgrowing the supply, putting added pressure on Chinese decision-makers
C2	China establishes Special Economic Zones in 2006[166]	1	0	These zones are designed to increase foreign investment, but lead to more favorable terms that make Chinese services more competitive
C3	Chinese military support has led to unstable governments remaining in power[167]	1	0	China trades military weapons to unstable regimes leading to those governments staying in power, but has yet to come back and haunt the Chinese or alter decison making
C4	Chinese open military base in Djibouti in 2017[168]	1	1	This is the first overseas base for the PLA, giving its military extended reach and capabilities in Africa
C5	Chinese companies underbid infrastructure contracts[169]	1	1	Chinese underbid US contracts by 40% to gain access to untapped markets
C6	China becomes key trade partner in Africa[170]	1	1	From 2000-2012, China increased from approximately $10 billion to $200 billion; representing a 13% share as compared to 8% for the US

[165] Hanauer and Morris, *Chinese Engagement in Africa,* 35.

[166] Ibid., 39.

[167] Ibid., 45.

[168] Dr. Indu Saxena, Robert Uri Dabaly, and Arushi Singh, "China's Military and Economic Prowess in Djibouti: A Security Challenge for the Indo-Pacific," *Journal of Indo-Pacific Affairs:Africa in the Indo-Pacific Construct* 4, no. 8 (Special Issue November 2021): 112.

[169] Feldstein, *Testimony before the U.S.-China Economic and Security Review Commission,* 10.

[170] Hanauer and Morris, *Chinese Engagement in Africa,* 26.

C7	China increases support to UN peacekeeping missions[171]	1	1	China went from 27 personnel supporting in 2001 to over 1800 in 2012; the largest number for any one country and gives China the ability to dictate operations
C8	China successfully eases tensions in South Sudan[172]	1	1	China leveraged its diplomatic and economic clout to bring both sides to the table and gained a better relationship with both parties as a result
C9	China is the largest contributor to UN peacekeeping missions[173]	1	1	China uses these missions to give its military operational experience
C10	China impedes UN investigation into arms sales in Africa[174]	2	0	China continues to hamper the UN from looking into Chinese secret deals that end with Chinese weapons ending up in the hands of rebel groups which could have negative impacts on Africa's perception of China
C11	In 2018, Chinese get Djibouti's government to restrict airspace over China's base[175]	2	0	To protect its interests and secrets, China restricts the US from flying over its base in Djibouti
C12	Djibouti clamping down on Chinese dissent[176]	2	0	Most of the citizens of Djibouti are not feeling the impacts of China's investments and have begun questioning what the government is doing with the money so China has moved to suppress the dissent
C13	China has created thousands of unskilled labor jobs[177]	3	-1	However, all management positions are held by Chinese, with little chance of succession for Africans; Chinese import workers, and Chinese are paid more which tells most African's they will never be more than unskilled laborer

[171] Ibid., 44.

[172] Hanauer and Morris, *Chinese Engagement in Africa,* 84.

[173] Ibid., 9.

[174] Ibid., 41.

[175] Vertin, *Great Power Rivalry in the Red Sea,* 8.

[176] Ibid., 12.

[177] Hanauer and Morris, *Chinese Engagement in Africa,* 48.

C14	Chinese investments invite African corruption[178]	3	-1	A lack of general oversight leads to China giving government officials kickbacks to get deals done
C15	Increased Chinese presence leads to tensions[179]	3	-1	Many Chinese migrants are seen as of symbols of Chinese intervention where it is not wanted; often Chinese do not assimilate
C16	In 2009, China invested $6.6 billion dollars towards expanding Chinese media in Africa	3	0	China seeks to promote Chinese culture in Africa
C17	In 2012, state run Chinese Central TV (CCTV) established CCTV Africa	3	0	China seeks to promote Chinese culture in Africa
C18	In 2012, China Daily (largest English Newspaper) establishes launches first African edition[180]	3	0	China seeks to promote Chinese culture in Africa
C19	China trains African students	3	1	This gives China unfettered access to shape Africa's next generation
C20	China prioritizes Africa through diplomatic visits[181]	3	1	China shows great importance for Africa by sending senior level officials on their first international visits; and President Jinato has even visited more countries in Africa than the South African President
C21	President Xi visits Africa on first trip in 2013[182]	3	1	President Obama visited the same countries months later, giving the perception that the US was playing catch-up
C22	China floods Africa with cheap goods made in China[183]	4	-1	The influx of Chinese goods has put hundreds of thousands of Africans out of work which influences dissent in portions of Africans that are affected

[178] Ibid., 50.

[179] Hanauer and Morris, *Chinese Engagement in Africa*, 54.

[180] Ibid., 74.

[181] Ibid., 45.

[182] Ibid., 46.

[183] Ibid., 15.

C23	China debt traps[184]	4	-1	Increasing Chinese debt creates inviable economic situations and high levels of official corruption which can negatively affect Chinese influence
C24	Chinese projects criticized for poor quality	4	-1	Chinese built hospital closes after four years due to structure defects leading to negative perception of Chinese projects
C25	Chinese projects criticized for poor quality	4	-1	Chinese built road washes away after first rainy season leading to negative perception of Chinese projects
C26	Chinese projects criticized for poor quality	4	-1	South Africa have trouble dealing with Chinese company repairing power grid leading to negative perception of Chinese projects
C27	China invests little into social infrastructure[185]	4	-1	China mainly uses Africans for unskilled labor, cut health care benefits, and reduced public utilities support which created public dissent against these policies
C28	China often pays below minimum wage[186]	4	-1	This has led to violent protests in Zambia
C29	China financed and built over 70% of Africa's digital infrastructure[187]cyber ops	4	0	China is positioned to shaped how Africans communicate, do business, and access public services
C30	Many African countries trade at a deficit with China[188]	4	0	Countries that do not possess natural resources acquire debt to trade with China, leaving them vulnerable to Chinese economic influence
C31	African support for China decreases as Chinese imports increase[189]	4	0	Chinese imports causing non-competitive industries to close; eliminating thousands of jobs for Africans which causes negative perceptions of China

[184] Ibid., 45.

[185] Hanauer and Morris, *Chinese Engagement in Africa,* 63.

[186] Ibid., 66.

[187] Rebecca Arcesati, "China's Evolving Role in Africa's Digitalisation: From Building Infrastructure to Shaping Ecosystems," Italian Institute for International Political Studies, 29 July 2021, https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247.

[188] Hanauer and Morris, *Chinese Engagement in Africa,* 31.

[189] Ibid., 62.

C32	China is seeking to grow its global influence through soft power[190]	4	0	China has acknowledged that it is fighting an uphill battle against western cultural ideals in Africa
C33	China increases military cooperation with African countries[191]	4	0	This is partially due to an increase in tensions against Chinese nationals who needed protection
C34	Djibouti debt to GDP ratio goes from 34% to as high as 104% in 2018, with China as the largest owner of these debts[192]	4	0	This leaves countries like Djibouti highly reliant on outside forces to maintain and are highly vulnerable to events like COVID-19 that shut economies down
C35	Chinese aid is tied to procurement of Chinese goods and services[193]	4	0	Exemplified by clauses such as, no less than 50% of aid must be procured from China or country must recognize the One China policy
C36	African leaders claim credit for delivering services funded by China[194]	4	1	African regimes rely on Chinese funding to remain in power and is a source of influence over them
C37	Malawi recognizes One China Policy in 2008[195]	4	1	Malawi immediately receiving infusion of aid after recognizing 'One China' policy shows Chinese influence in political decisions
C38	China treats African leaders as partners[196]	4	1	China emphasizes equality with African leaders which is not often reciprocated by Western leaders
C39	China deals with unstable countries such as South Sudan and Democratic Republic of Congo[197]	4	1	China invests in countries that the West is unwilling to work with giving them unmatched influence in those countries
C40	China trains African students[198]	4	1	This gives China unfettered access to influence Africa's next generation

[190] Ibid., 79.

[191] Ibid., 86.

[192] Vertin, *Great Power Rivalry in the Red Sea*, 13.

[193] Hanauer and Morris, *Chinese Engagement in Africa*, 38.

[194] Ibid., 3.

[195] Ibid., 7.

[196] Ibid., 10.

[197] Ibid., 12.

[198] Ibid., 16.

C41	Perception that more of China's aid dollars go towards aid projects[199]	4	1	China has influenced African leaders that China is more fiscally responsible with aid than Western aid workers
C42	China leverages influence in Africa with UN resolutions[200]	4	1	China uses its seat on the UN security council to show perception of working to create peaceful resolutions in Africa
C43	China has increased infrastructure investment[201]	4	1	Investment went from $500 million in 2001 to $14 billion in 2011 which gives them unmatched influence
C44	China uses future revenue as collateral for loans[202]	4	1	China preys on resource rich countries to trade infrastructure development for natural resources which can influence that country's future decisions
C45	China uses developmental assistance as an influence tool[203]	4	1	With nearly half of its global aid dollars going to Africa, China leverages its assistance programs to counteract any negative perceptions of Chinese activities in Africa
C46	China conducts high level Military visits to Africa; hosts visits to China[204]	4	1	Many high level African military leaders receiving training in China which influences them to work closer with China in the future
C47	President of Zambia runs campaign on expelling China from country[205]	4	1	Immediately changes tune upon being elected
C48	China conducts cultural exchanges[206]	4	1	China is working to enhance its relationship and perception with Africans
C49	As of 2012, China has built 31 Confucius institutes and five Confucius classrooms	4	1	China is attempting to spread the Chinese language and culture to orient Africans towards China

[199] Ibid.

[200] Ibid., 23.

[201] Hanauer and Morris, *Chinese Engagement in Africa*, 34.

[202] Ibid., 35.

[203] Ibid., 36.

[204] Ibid., 42.

[205] Ibid., 55.

[206] Ibid., 76.

	across 26 African countries[207]			
C50	Chinese projects increased Djibouti's GDP from $1.3 billion in 2012 to $3.1 billion in 2019[208]	4	1	China leveraged its economic influence in opening up its first overseas military base in 2017
C51	China trains African journalists[209]	4	1	China brings African journalists to China and treats them royally; example is 22 Zambian journalists came back from China with glowing reports and Chinese propaganda threaded into articles
C52	China builds surveillance networks in several African countries[210]	5	0	Gives China numerous opportunities to leverage access to these networks
C53	DRS started in 2015, have launched satellites and laid fiber for 30 African countries[211]	5	0	China owns such a large portion of the information infrastructure it can conceivably control African communications
C54	Installed hundreds of safe cities across Africa[212]	5	0	Under the guise of safety, China has installed surveillance equipment despite concerns over human rights and security of equipment, which gives China further access to create technical advantages in Africa
C55	China has access to unlimited data from Chinese built infrastructure[213]	5	0	While it denies doing so, China has access to all of Africa's data for information and intelligence purposes

[207] Ibid., 78.

[208] Vertin, *Great Power Rivalry in the Red Sea*, 9.

[209] Paul et al., *A Guide to Extreme Competition with China*, 20.

[210] Feldstein, *Testimony before the U.S.-China Economic and Security Review Commission,* 1.

[211] Paul et al., *A Guide to Extreme Competition with China*, 21.

[212] Ibid., 22.

[213] Woodhams, "How China Exports Repression to Africa: China's 'Techno-dystopian Expansionism' is Undermining Democracy in African Countries."

C56	China spreading censorship of internet[214]	5	0	As China works to build Africa's digital infrastructure, it is enabling pariah governments to suppress any public dissent
C57	China develops Digital Silk Road (DRS) Initiative in 2015[215]	5	1	Five countries in Africa have signed on worth a combined $8.43 Billion
C58	China trains Africans on cyber security[216]	5	1	This program is similar to the journalists training and leads to a close relationship between Chinese and African cyber experts
C59	China using Africa to build its database to increase its Artificial Intelligence capabilities[217]	5	1	China is able to diversify its data and expand its AI programs

[214] Nick Bailey, "East African States Adopt China's Playbook on Internet Censorship," Freedom House, October 24, 2017, https://freedomhouse.org/article/east-african-states-adopt-chinas-playbook-internet-censorship.

[215] Feldstein, *Testimony before the U.S.-China Economic and Security Review Commission,* 2.

[216] Paul et al., *A Guide to Extreme Competition with China*, 21.

[217] Samuel Woodhams, "How China Exports Repression to Africa: China's 'Techno-dystopian Expansionism' is Undermining Democracy in African Countries."

APPENDIX B

CHAPTER 4 RESULTS (RUSSIA)

#	Action	IA LOE	Assessment	Notes
R1	Information troops were the main effort for Russia[218]	1	0	Russia used its information capabilities to recruit more people to its efforts and is the primary tool in its aggressive actions against the Ukraine
R2	Russia moved to immediately control telecommunications infrastructure[219]	1	1	Control of Ukrainian infrastructure allowed for SIGINT collection which enabled Russian follow-on operations
R3	Pro-Russian management did not immediately cut off communication traffic through compromised networks[220]	1	1	This allowed Russia to gain access to internal Ukrainian systems giving Russia maximum intelligence gathering
R4	Russia isolates Donbass from the rest of Ukraine[221]	1	1	Through physical attack and cyber means, Russia cut access to outside broadcasts, communication networks, and ability to send or receive money to enable maneuver on the ground
R5	Russia leverages Signals Intelligence (SIGINT) in targeting[222]	1	1	Russian leveraged its access to Ukrainian networks to lethally target the Ukrainian military
R6	Russia utilizes hybrid warfare to confront Western powers[223]	1	1	Russia utilized disinformation deception to compensate for its relative military weakness in relation to Western powers
R7	Russia never *"*declared war*"*[224]	1	1	Russia utilized deception in sending the *"*little green men*"* without declaring war, giving Russia the initial advantage in blockading most of the Crimean military bases without intervention

[218] Snegovaya, *Putin's Information Warfare in Ukraine,* 15.

[219] Pakharenko, "Cyber Operations at Maidan," 62.

[220] Ibid.

[221] Ibid.

[222] Ibid., 63.

[223] Snegovaya, *Putin's Information Warfare in Ukraine,* 11.

[224] Ibid., 11.

#	Action	IA LOE	Assessment	Notes
R8	Russian senior officials leveraged disinformation in its dealings concerning operations in Ukraine[225]	1	1	No one knew Russia's goals in Ukraine, the number of troops is still unknown; giving the Russians the advantage of ambiguity as NATO allies were unable to act without clear proof of Russian actions
R9	Russia was able to legally never be involved in the conflict[226]	1	1	This allowed Russia to be a part of the peace talks as a third party; allowing it to escape any responsibility for keeping the agreement
R10	Russia synchronized cyber and EW with physical movement[227]	1	1	Russia maximized the effectiveness of its cyber and EW by directly linking it with actual actions on the ground
R11	Pro-Russian government leaders shut off TV, phones, and internet of main opposition[228]	2	0	Russia sought to silenced anyone who spoke out against the Russian backed government
R12	Russia leverages several various forms of cyber to obfuscate attribution[229]	2	0	Russia constantly used various actors, tools, and tactics to utilizes liminal warfare to stay below the attribution threshold
R13	Russia leveraged deception to gain tactical advantages[230]	2	0	While this obfuscated the time and place of their movement, these same tactics will likely prove less beneficial if tried again
R14	Russia utilized disinformation to obfuscate size of force on border[231]	2	1	Ukraine and Western allies were unable to determine the size or intentions of the Russian force on the border prior to incursion

[225] Snegovaya, *Putin's Information Warfare in Ukraine,* 15.

[226] Ibid., 16.

[227] Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2 (Summer 2017): 54.

[228] Pakharenko, "Cyber Operations at Maidan," 61.

[229] Ibid., 63.

[230] Snegovaya, *Putin's Information Warfare in Ukraine,* 17.

[231] Ibid., 9.

#	Action	IA LOE	Assessment	Notes
R15	Using reflexive control, Russia blames conflict on the US and NATO allies[232]	3	0	Russia sought to change the narrative by claiming it had evidence to show NATO was the real threat to Ukraine, not Russia
R16	Russian strategic communications were proactive in messaging its supporters, both domestically and in Ukraine[233]	3	0	This helped to provide justification to its population for its actions and promote Russia as the answer for providing for ethnic Russian needs in Ukraine
R17	Russia spins Malaysian Airlines flight 17 tragedy[234]	3	0	Russian attempted to spin a narrative that the plane was shot down and staged by Ukrainian military, which no one outside of Russia believed
R18	Russian disinformation was largely unsuccessful in targeting civilian populations outside of Russia and Ukraine[235]	4	-1	Russia was unable to sway international opinion for those exposed to a wider source of news; in fact, made Russia more isolated
R19	Russia activated social network groups to push pro-Russian propaganda[236]	4	0	Russia used these groups to push and alter articles covering the events in Ukraine which had mixed results
R20	Russia uses mirroring tactics against opposition[237]	4	0	Russia believed that if they could mimic the opposition, it would lead them to a predetermined outcome be able to more effectively influence them
R21	Russia labeled the 'Banderite' government as illegitimate[238]	4	0	Russia utilized the media and diplomatic sources to incessantly message against the legitimacy of the Ukrainian government

[232] Timothy Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, KS, Foreign Military Studies Office, 2015), 388.

[233] Iasiello, "Russia's Improved Information Operations," 57.

[234] Ed Adamczyk, "Russia Offers Alternate Scenarios for Malaysia Airlines Crash," *UPI,* July 22, 2014, https://www.upi.com/Top_News/World-News/2014/07/22/Russia-offers-alternate-scenarios-for-Malaysia-Airlines-crash/2701406045751/.

[235] Snegovaya, *Putin's Information Warfare in Ukraine,* 19.

[236] Pakharenko, "Cyber Operations at Maidan," 62.

[237] Snegovaya, *Putin's Information Warfare in Ukraine,* 10.

[238] Ibid., 12.

#	Action	IA LOE	Assessment	Notes
R22	Russia sought to drive wedges between NATO countries[239]	4	0	Russia's goal was to disunify any response from NATO, thus making them appear weak which worked only in the short term
R23	Russia sent text messages to Ukrainian soldiers[240]	4	0	Russia attempted to with little success to demoralize Ukrainian troops through text messages about running from inevitable death
R24	Russia paid for people to pose as multiple people online personas to spread mis/disinformation[241]	4	0	Russia leveraged internet trolls to amplify their message; while not always effective, it did serve to create confusion, if only temporarily
R25	Russia leaked phone calls of US officials[242]	4	0	Russia used disinformation to embarrass US into inaction
R26	Russia sought to exacerbate Ukrainian issues to its advantage[243]	4	1	This gave Russia the ability to pick and choose how to exploit Ukrainian weaknesses to their advantage
R27	Russian senior leaders deny any military actions in Ukraine[244]	4	1	Russia continuously denied any military occupation in Ukraine which is straight out of its disinformation handbook, which gave them the ability to take part in the peace talks
R28	Russia exerted diplomatic pressure to stop Ukraine from joining the EU in 2013[245]	4	1	Russia threatened repercussions if Ukraine joined the EU, showing its desire to keep the old Soviet Bloc under its control

[239] Snegovaya, *Putin's Information Warfare in Ukraine,* 14.

[240] Duncan McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine," *The RUSI Journal* 165, no. 7 (November 2020): 34-44, https://www.tandfonline.com/loi/rusi2037.

[241] Iasiello, "Russia's Improved Information Operations," 56.

[242] Ibid., 57.

[243] Snegovaya, *Putin's Information Warfare in Ukraine,* 12.

[244] Ibid., 15.

[245] Rikard Jozwiak, "After Kyiv Snub, Kwasniewski Says EU-Ukraine Deal Is Off," *Radio Free Europe,* November 21, 2013, https://www.rferl.org/a/ukrainetymoshenko-bill-rejected/25175222.html.

#	Action	IA LOE	Assessment	Notes
R29	Russia conducted large scale exercises on the border[246]	4	1	These exercises were leveraged psychological pressure and condition NATO to large troop numbers on the border
R30	Russia used a mixture of truth and lies to influence Ukrainian political process[247]	4	1	Russia sought to maintain political influence over Ukraine by whatever meanscreating chaos and exploiting the political divide
R31	Russia leveraged ethnic Russians to support efforts in Ukraine[248]	4	1	Russia leveraged their ties to Russiathe diaspora to act as a proxy for Russian actions to spread chaos in Ukraine
R32	Russia invested and used Electromagnetic Warfare (EW) heavily in Ukraine, learning from mistakes in Georgia[249]	5	0	Russian leaders believed that starting a war without control of the electromagnetic spectrum was inviting inevitable defeat;
R33	Russia disrupted Ukrainian radio transmissions with EW[250]	5	0	Russia dominated the electronic battlefield in Ukraine in the early phases of the conflict until Ukraine changed their security measures
R34	Russia targets Ukraine with Distributed Denial of Service (DDoS) attacks[251]	5	1	DDoS attacks focused on Ukrainian political and economic websites; shutting them down for an extended period and disrupted Ukrainian government
R35	Russia use cyber tools to target protestors late 2013[252]	5	1	Russia targeted key opposition through cyber means to plant evidence and get them arrested

[246] Ian Brezezinski and Nicholas Sarangis, "The NATO-Russia Exercise Gap," *NATO Source* (blog), *The Atlantic Council*, October 26, 2017, http://www.atlanticcouncil.org/blogs/natosource/the-nato-russia-exercise-gap.

[247] Alya Shandra and Robert Seely, "The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine," (Occasional Paper, Royal United Services Institute for Defence and Security Studies, London, UK, July 2019), 35, https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf.

[248] Iasiello, "Russia's Improved Information Operations," 54.

[249] McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine."

[250] Ibid., 36.

[251] Pakharenko, "Cyber Operations at Maidan," 59.

[252] Ibid., 61.

#	Action	IA LOE	Assessment	Notes
R36	Russia disrupted opposition parliament members cell phones[253]	5	1	Constantly messaged and called opposition phones so they were unable to communicate immediately following a lethal event at a protest
R37	Russia moved to immediately control telecommunications infrastructure[254]	5	1	Russia immediately gained physical access to infrastructure, severing cables routing all Ukrainian communications through Russian operators
R38	Russia constantly attacks Ukrainian critical infrastructure through cyber means[255]	5	1	Russia hires mercenaries to constantly probe for vulnerabilities in Ukrainian networks
R39	Much of Ukraine infrastructure is Russian made[256]	5	1	Russia built, then exploited vulnerabilities in Ukraine networks
R40	EW caused Ukrainians to use cell phones[257]	5	1	Cell phone use made it easier for Russians to target Ukrainians

[253] Pakharenko, "Cyber Operations at Maidan," 61.

[254] Ibid., 62.

[255] Ibid., 63.

[256] Ibid., 65.

[257] McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine," 37.

BIBLIOGRAPHY

Adamczyk, Ed. “Russia Offers Alternate Scenarios for Malaysia Airlines Crash.” *UPI.* July 22, 2014. https://www.upi.com/Top_News/World-News/2014/07/22/Russia-offers-alternate-scenarios-for-Malaysia-Airlines-crash/2701406045751/.

Alexander, Keith B., and Jamil N. Jaffer. “Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition.” *Georgetown Journal of International Affairs* 19 (Fall 2018): 51-66. http://www.jstor.org/stable/26567527.

Arcesati, Rebecca. “China’s Evolving Role in Africa’s Digitalisation: From Building Infrastructure to Shaping Ecosystems.” Italian Institute for International Political Studies. July 29, 2021. https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247.

Bailey, Nick. “East African States Adopt China’s Playbook on Internet Censorship.” Freedom House. October 24, 2017. https://freedomhouse.org/article/east-african-states-adopt-chinas-playbook-internet-censorship.

Ball, Deborah Yarsike. “Protecting Falsehoods With a Bodyguard of Lies: Putin’s Use of Information Warfare.” Research Paper No. 136, Research Division, NATO Defense College, Rome, February 2017. https://www.ndc.nato.int/news/news.php?icode=1017.

Bebber, Robert J. “Treating Information as a Strategic Resource to Win the ‘Information Warfare’.” *Orbis* 61, no. 3 (2017): 394-403. https://www.sciencedirect.com/science/article/abs/pii/S0030438717300492?via%3Dihub.

Bokel, John. “Information as an Instrument and a Source of National Power.” Paper, The Industrial College of the Armed Forces, National Defense University, Fort McNair, Wasington, DC, 2003. https://apps.dtic/sti/pdfs/ADA422060.pdf.

Booz, Allen, Hamilton. *The Future of Africa: Th Future of China in Africa 2035.* Final Report, Final Deliverable. Prepared for Director, Net Assessment, Office of the Secretary of Defense. Washington, DC: Booz Allen Hamilton, June 2014.

Brands, Hal, and Tim Nichols. “Special Operations Forces and Great-Power Competition in the 21st Century.” American Enterprise Institute, Washington, DC, August 04, 2020. https://www.aei.org/research-products/report/special-operations-forces-and-great-power-competition-in-the-21st-century/.

Brezezinski, Ian, and Nicholas Varangis. “The NATO-Russia Exercise Gap.” *NATO Source* (Blog). *The Atlantic Council,* October 26, 2017. http://www.atlanticcouncil.org/blogs/natosource/the-nato-russia-exercise-gap.

Cheng, Dean. “Winning Without Fighting: The Chinese Psychological Warfare Challenge.” (Backgrounder No. 2821, The Heritage Foundation, Washington, DC, 2013). https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

Clarke, Richard. “Statement of General Richard D. Clarke, US Army Commander, United States Special Operations Command, before the House Armed Services Committee; Intelligence, Emerging Threats and Capabilities Subcommittee.” Washington, DC, April 09, 2019. https://armedservices.house.gov/_cache/files/7/9/7970f176-0def-4a2d-beb3-a7d5d69e513b/9C80F888EEE40D8E82ABFF5336C012C3.hhrg-116-as26-wstate-clarker-20190409.pdf.

Croot, Edward. “There Is an Identity Crisis in Special Forces: Who Are the Green Berets Supposed to Be?” Fellows Strategy Research Project, US Army War College, January 03, 2020. https://sites.duke.edu/tcths_fellows/files/2020/04/Ed-Croot-Final-Paper.pdf.

Davis, Norman C. “An Information-based Revolution in Military Affairs.” In *In Athena’s Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla, and David Ronfeldt, 79-98. Washington, DC: Rand Corporation, 1997. https://www.jstor.org/stable/10.7249/mr880osd-rc.9?seq=1.

Dougherty, Chris. “Confronting Chaos: A New Concept for Information Advantage.” *War on the Rocks*, September 21, 2021. https://warontherocks.com/2021/09/confronting-chaos-a-new-concept-for-information-advantage/.

Fabrizio, Kira, and David Mowery. “Defense-Related R&D and the Growth of the Postwar Information Technology Industrial Complex in the United States.” *Revue d’économie industrielle* 112, no. 4 (2005): 27-44. https://www.persee.fr/doc/rei_0154-3229_2005_num_112_1_3123.

Feickert, Andrew. “Defense Primer: Army Multi-Domain Operations (MDO).” Congressional Research Service, Washington, DC, updated October 22, 2021. https://sgp.fas.org/crs/natsec/IF11409.pdf.

Feldstein, Steven. *Testimony before the US-China Economic and Security Review Commission Hearing on China’s Strategic Aims in Africa*. Washington, DC, May 8, 2020. https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.

Gambill, Jason. “China and Russia Are Waging Irregular Warfare Against the United States: It Is Time for a US Global Response, Led by Special Operations Command.” Joint Intermediate Force Capabilities Office, November 15, 2021. https://jnlwp.defense.gov/Press-Room/In-The-News/Article/2857039/china-and-russia-are-waging-irregular-warfare-against-the-united-states-it-is-t/.

Garamone, Jim. “Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence.” *DoD News.* June 2, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2641068/official-talks-dod-policy-role-in-chinese-pacing-threat-integrated-deterrence/.

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

Giles, Keir. *Handbook of Russian Information Warfare*. Fellowship Monograph 9. Rome: Research Division, NATO Defense College, November 2016. https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf.

Guangoian, Peng, and Yao Youzhi, eds. *The Science of Military Strategy.* Beijing: National Military Science Publishing House, 2005.

Hammerstrom, Michael. “Delivering the Information Advantage.” PowerPoint Presentation, TechNet, Cyber Center of Excellence, Augusta, GA, 2021. https://events.afcea.org/Augusta21/Custom/Handout/Speaker0_Session8922_1.pdf.

Hanauer, Larry, and Lyle J. Morris. *Chinese Engagement in Africa Drivers, Reactions, and Implications for US Policy.* Santa Monica, CA: Rand Corporation, 2014. https://www.rand.org/pubs/research_reports/RR521.html.

Hayes, III, James E.. “Beyond the Gray Zone: Special Operations in Multidomain Battle.” *Joint Force Quarterly* 91 (4th Quarter 2018): 60-66. https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=1&sid=4d70a56a-2db7-4ee3-9428-8df177fe8532%40redis.

Headquarters, Department of the Army. Army Doctrine Publication 3-05, *Army Special Operations.* Washington, DC: Army Publishing Directorate, 2019.

Hirvela, Arto. “Thoughts of War Theorists on Information Operations.” Paper presented at European Conference on Information Warfare & Security, Helsinki, Finland, 2011. https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/detail/detail?vid=2&sid=540fdbd3-73e0-4d33-ab6b-88dffdefd4d3%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=67467530&db=tsh.

Iasiello, Emilio J. “Russia’s Improved Information Operations: From Georgia to Crimea.” *Parameters* 47, no. 2 (Summer 2017): 51-63.

Jozwiak, Richard. “After Kyiv Snub, Kwasniewski Says EU-Ukraine Deal Is Off.” *Radio Free Europe,* November 21, 2013. https://www.rferl.org/a/ukrainetymoshenko-bill-rejected/25175222.html.

Kalha, R. S. “An Assessment of the Chinese Dream: 2015.” *Strategic Analysis* 39, no. 3 (2015): 274-279. https://www.tandfonline.com/doi/full/10.1080/09700161.2015.1022317.

Kania, Elsa B., and John K. Costello. “The Strategic Support Force and the Future of Chinese Information Operations.” *The Cyber Defense Review* 3, no. 1 (Spring 2018): 105-122. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf.

Keohane, Robert, and Joseph Nye, Jr. “Power and Interdependence in the Information Age.” *Foreign Affairs* 77, no. 5 (September-October 1998): 81-94. https://www-jstor-org.jsou.idm.oclc.org/stable/20049052?seq=6.

Kilcullen, David. *The Dragons and the Snakes: How the Rest Learned to Fight the West.* New York, NY: Oxford University Press, 2020.

Larew, Karl G. “From Pigeons to Crystals: The Development of Radio Communication in US Army Tanks in World War II.” *Historian* 67, no. 4 (2005): 664-677. https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=6&sid=1294c4c9-9a21-4ff7-b300-a49b19f31f2b%40redis.

Larrabee, Stephen F., Peter A. Wilson, and John Gordon, IV. *The Ukrainian Crisis and European Security: Implications for the United States and US Army*. Santa Monica, CA: Rand Corporation, 2015. https://www.rand.org/pubs/research_reports/RR903.html.

Latvian Institute of International Affairs. *Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia.* Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016. https://stratcomcoe.org/publications/internet-trolling-as-a-hybrid-warfare-tool-the-case-of-latvia/160.

Lehrer, Christiane, Alexander Wieneke, Jan vom Brocke, Reinhard Jung, and Stefan Seidel. “How Big Data Analytics Enables Service Innovation: Materiality, Affordance, and the Individualization of Service.” *Journal of Management Information Systems* 35, no. 2 (2018): 424-460.

Leonhard, Robert R. *The Principles of War for the Information Age.* New York: Ballentine Books, 1998.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare: China’s Master Plan to Destroy America.* Panama City, Panama: Pan American Publishing Company, 1999.

Libicki, Martin. “The Convergence of Information Warfare.” *Strategic Studies Quarterly* 11, no. 1 (Spring 2017): 49-65. https://www-jstor-org.jsou.idm.oclc.org/stable/26271590?seq=1.

Lin, Herb. “A Hypothetical Command Vision Statement for a Fictional PLA Cyber Command.” *Cybersecurity and Deterrence* (Blog). *Lawfare.* October 22, 2021. https://wwww.lawfareblog.com/hypothetical-command-vision-statement-fictional-pla-cyber-command.

Mason, Jessica. “What Is Information Warfare and How Is It Different from Traditional Warfare.” Social Media Writings, Aalto University, December 05, 2019. https://medium.com/social-media-writings/what-is-information-warfare-and-how-is-it-different-from-traditional-warfare-a42294ae8c8d.

McBride, Andrew, and James Chatzky. “China’s Massive Belt and Road Initiative.” Council on Foreign Relations. Last updated January 28, 2020. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

McCrory, Duncan. “Russian Electronic Warfare, Cyber and Information Operations in Ukraine.” *The RUSI Journal* 165, no. 7 (November 2020): 34-44. https://www.tandfonline.com/loi/rusi20.

McIntosh, Scott. “The Wingman-Philosopher of MiG Alley: John Boyd and the OODA Loop.” *Air Power History* 58, no. 4 (Winter 2011): 24-33. https://www-jstor-org.jsou.idm.oclc.org/stable/26276108.

McLynn, Frank. “The Brutal Brilliance of Chengis Khan.” *History Extra.* February 22, 2019. https://www.historyextra.com/period/medieval/the-brutal-brilliance-of-genghis-khan/.

Merriam-Webster, Incorporated. “Information.” Merriam-Webster. Accessed April 11, 2022. https://www.merriam-webster.com/dictionary/information.

Miller, Joe, Monte Erfourth, Jeremiah Monk, and Ryan Oliver. “Harnessing David and Goliath: Orthodoxy, Asymmetry, and Competition.” *Small Wars Journal.* February 07, 2019. https://smallwarsjournal.com/jrnl/art/harnessing-david-and-goliath-orthodoxy-asymmetry-and-competition.

Ministry of Defence of the Russian Federation. “Mission and Objectives of the Russian Armed Forces.” Accessed January 06, 2022. https://eng.mil.ru/en/mission/tasks.htm.

Morrison, J. Stephen, Jennifer Cooke, Indira Campos, Michael Chege, Pat Utomi, and Alex Vines. *US and Chinese Engagement in Africa: Prospects for Improving US-China-Africa Cooperation.* Washington, DC: Center for Strategic & International Studies, July 2008.

Mulholland, Jr., John F. “Countering Irregular Threats: The Army Special Operations Contribution.” *Joint Force Quarterly* 56 (1st Quarter 2010): 71-75.

Office of the Chairman of the Joint Chiefs of Staff. Joint Publication 3-0, *Joint Operations.* Washington, DC: Joint Chiefs of Staff, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/docnet/jp30/story_content/external_files/jp3_0_20170117%20(1).pdf.

———. Joint Publication 3-13, *Information Operations.* Washington, DC: Joint Chiefs of Staff, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. Joint Publication 3-24, *Counterinsurgency.* Washington, DC: Joint Chiefs of Staff, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_24.pdf.

———. Joint Publication 5-0, *Joint Planning*. Washington, DC: Joint Chiefs of Staff, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf.

Pacepa, Ion Mihai, and Ronald J. Rychlak. *Disinformation.* Washington, DC: WND Books, Inc., 2013.

Pakharenko, Glib. “Cyber Operations at Maidan: A First-Hand Account.” In *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers, 59-66. Tallinn: NATO CCD COE Publications, 2015. https://ccdcoe.org/uploads/2018/10/Ch07_CyberWarinPerspective_Pakharenko.pdf.

Paul, Christopher. “Understanding and Pursuing Information Advantage.” *Cyber Defense Review* 5, no. 2 (Summer 2020): 109-124. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Paul_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053231-950#:~:text=A%20position%20of%20relative%20advantage%20is%20a%20location,risk%20and%20move%20to%20a%20position%20of%.

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding. *Lessons from Others for Future US Army Operations in and Through the Information Environment.* Santa Monica, CA: Rand Corporation, 2018.

Paul, Christopher, James Dobbins, Scott W. Harold, Howard J. Shatz, Rand Waltzman, and Lauren Skrabala. *A Guide to Extreme Competition with China.* https://www.rand.org/pubs/research_reports/RRA1378-1.html, Santa Monica, CA: Rand Corporation, 2021.

Paul, Christopher, and Michael Schwille. “The Evolution of Special Operations as a Model for Information Forces.” *Joint Forces Quarterly* 100 (1st Quarter 2021): 8-13. https://eds-s-ebscohost-com.jsou.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=2&sid=bc1698ca-8615-49c1-940d-bd845193df09%40redis, 8-13.

Pelaez, Mark. “Hearts and Minds as Targets: PSYOP ANCOC Trains Inside the Box, but Thinks Outside of It, Too.” *Special Warfare* 22, no. 4 (July 2009): 22-24. https://search-ebscohost-com.jsou.idm.oclc.org/login.aspx?direct=true&db=tsh&AN=44061376&site=eds-live.

Pisnia, Natalka. “Why Has RT Registered as a Foreign Agent with the US?” *BBC News*, November 15, 2017. https://www.bbc.com/news/world-us-canada-41991683.

Pomerantsey, Peter. “Russia and the Menace of Unreality.” *The Atlantic*, September 14, 2014. https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

Pomerleau, Mark. “Army to Set in Stone the Importance of Information Advantage.” *C4ISRNet,* July 01, 2021. https://www.c4isrnet.com/information-warfare/2021/07/01/army-to-set-in-stone-the-importance-of-information-advantage-with-new-capabilities-on-deck/.

———. “A New Name-and Focus-for Army Cyber Command?” *C4ISRNet,* August 21, 2019. https://www.c4isrnet.com/show-reporter/technet-augusta/2019/08/21/a-new-name-and-focus-for-army-cyber-command/.

———. “Why Is the United States Losing the Information War?” *C4ISRNet,* October 05, 2020. https://www.c4isrnet.com/information-warfare/2020/10/05/why-is-the-united-states-losing-the-information-war/.

Saxena, Dr. Indu, Robert Uri Dabaly, and Arushi Singh. “China’s Military and Economic Prowess in Djibouti: A Security Challenge for the Indo-Pacific.” *Journal of Indo-Pacific Affairs:Africa in the Indo-Pacific Construct* 4, no. 8 (Special Issue November 2021): 111-120.

Schaner, Eric X. “MCDP 8, Information: A New Marine Corps Doctrine for the information Warfighting Function.” *Marine Corps Gazette*, April 2022. https://mca-marines.org/wp-content/uploads/MCDP-8-Information.pdf.

Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China, 2011*. Washington, DC: Department of Defense, 2011. https://dod.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf.

———. *Summary of the 2018 National Defense Strategy: Sharpening the American Military’s Competitive Edge*. Washington, DC: Department of Defense, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Shandra, Alya, and Robert Seely. “The Surkov Leaks: The Inner Workings of Russia’s Hybrid War in Ukraine.” Occasional Paper, Royal United Services Institute for Defence and Security Studies, London, UK, July 2019. https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf.

Short, K.R.M. *Film and Radio Propaganda in World War II.* Knoxville: University of Tennessee Press, 1983.

Sinclair, Corey. “Russia’s Social Media i War in Ukraine.” Monograph, School of Advanced Military Studies, US .Army Command and General Staff College, May 2018. https://cgsc.contentdm.oclc.org/digital/collection/p4013coll3/id/4028/rec/3.

Singer, P. W., and Emerson Brooking. *Like War: The Weaponization of Social Media.* Boston: Houghton Mifflin Harcourt Publishing Company, 2018.

Snegovaya, Maria. *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. https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Steed, Brian L. “Narrative as a Critical Component for Violent Weaker Actor Success.” Ph.D. diss., University of Missouri-Kansas City, 2020. https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/74002/Steed_umkc_0134D_11583.pdf?sequence=1.

Sternhell, Yael A. “Communicating War: The Culture of Information in Richmond during the American Civil War.” *Past & Present*, no. 202 (February 2009): 175-205. http://www.jstor.org/stable/25580922.

Stronski, Paul, and Nicole Ng. *Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic.* Washington, DC: The Carnegie Endowment for Interational Peace, February 28, 2018. https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and%20china-in-central-asia-russian-far-east-and-arctic-pub-75673.

Teoli, Dac, Terrence Sanvictores, and Jason An. “SWOT Analysis.” National Center for Biotechnology Information, National Lirary of Medicine. Last updated September 08, 2021. https://www.ncbi.nlm.nih.gov/books/NBK537302/.

Thomas, Timothy L. “Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations.” *The Journal of Slavic Military Studies* 11, no. 1 (March 1998): 40-62.

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

US Marine Corps. Marine Corps Doctrine Publication 1, *Warfighting*. Washington, DC: Department of the Navy, Headquarters United States Marine Corps, 1997.

US President. *Interim National Security Strategic Guidance*. Washington, DC: The White House. March 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

Ukranian Election Task Force. *Foreign Interference in Ukraine's Election.* Washington, DC: The Atlantic Council, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/.

United States Army Special Operations Command (USASOC). *Army Special Operations Forces Strategy*. Fort Bragg, NC: USASOC, October 2019. https://www.soc.mil/AssortedPages/ARSOF_Strategy.pdf.

Vertin, Zach. *Great Power Rivalry in the Red Sea: China's Experiment in Djibouti and Implications for the United States.* Washington, DC: The Brookings Institution, June 2020. https://www.brookings.edu/wp-content/uploads/2020/06/FP_20200615_china_djibouti_vertin.pdf.

Watts, Stephen, Sean M. Zeigler, Kimberly Jackson, Caitlin McCulloch, Joseph Cheravitch, and Marta Keep. *Countering Russia: The Role of Special Operations Forces in Strategic Competition.* Santa Monica, CA: Rand Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA412-1.html.

Wei, Lingling. "China's New Power Play: More Control of Tech Companies' Troves of Data." *The Wall Street Journal*, June 12, 2021: https://www.wsj.com/articles/chinas-new-power-play-more-control-of-tech-companies-troves-of-data-11623470478.

Wilson, III, Isiah. "Rediscovering the Value of Special Operations." *Joint Forces Quarterly* 105 (2nd Quarter 2022): 37–43. https://search-ebscohost-com.jsou.idm.oclc.org/login.aspx?direct=true&db=asn&AN=156430039&site=eds-live.

Woodhams, Samuel. "How China Exports Repression to Africa: China's 'Techno-dystopian Expansionism' is Undermining Democracy in African Countries." *The Diplomat*, February 23, 2019. https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/.

Wortzel, Larry M. *The Chinese People's Liberation Army and Information Warfare*. Carlisle, PA: Strategic Sudies Institute and US Army War College Press, March 2014. https://publications.armywarcollege.edu/pubs/2263.pdf.

Zainal, Zaidah. "Case Study as a Research Method." *Jurnal Kemanusiaan*, 5, no. 1 (June 2007): 1-6. http://psyking.net/htmlobj-3837/case_study_as_a_research_method.pdf.