

COGNITIVE AND INFORMATION WARFARE IN THE NEW STRATEGIC REALITY:
EXAMINING THE NEED FOR UPGRADING U.S. OFFENSIVE AND DEFENSIVE
CAPABILITIES AGAINST MALIGN ADVERSARIES

A Master Thesis

Submitted to the Faculty

of

American Public University System

by

Sam Kessler

In Partial Fulfillment of the

Requirement for the Degree

of

Master of Arts, Intelligence Studies

With

Concentration in Intelligence Operations

April 2024

American Public University System

Charles Town, WV

The author hereby grants the American Public University System the right to display these contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by United States copyright law for the inclusion of any materials that are not the author's creation or in the public domain.

© Copyright 2024 by Sam Kessler

All rights reserved.

DEDICATION

I dedicate this thesis to my mom and dad, Barbara and Fred Kessler, for always reinforcing the importance of education and objective thinking throughout my life. Because of you I learned to explore my interests and passions that have helped me become well-rounded. You also taught me the value of persistence and staying the course when things get hard. I will forever be grateful for your constant love, support, and endless dedication as wonderful, caring, and loving parents.

ACKNOWLEDGMENTS

First, I would like to thank American Military University (AMU/APUS) for offering the online Masters Program in Intelligence Studies with Concentration in Intelligence Operations. This program was helpful and complimented my analytical background and previous Masters Program in National Security Studies with Concentration in Security and Intelligence Analysis with them. Combining operations and analysis were two priorities of mine and I'm thankful for the opportunity to work on that goal.

Secondly, I would like thank Dr. Al Lewis, my thesis professor, for his mentorship and guidance on tackling my thesis. His feedback and constructive criticism throughout the class and when reviewing my drafts were greatly appreciated. I would also like to thank each of my professors and fellow classmates since they all played a vital role in my learning experience at AMU. Since I'm originally an international affairs professional, I would also like to thank the Institute of International Studies at Bradley University where I received my B.A. in International Studies with a Minor in Economics.

Lastly, I would like to thank Max Daves for his friendship and seasoned insights as a national security and polymathic individual and for his legendary outside-the-box approach to solving problems. His discussions on spheres of influence and semiotics were inspired in the focus of this paper. I also wish to thank Beth Cresswell for our many talks on a wide range of topics and problems dealing with international and national security concerns, as well as sharing her passion and focus on human capital risk management that inspired me as well. I would also like to thank my fellow members at the Society for Defense and Strategic Studies (SDSS), a collegiate based organization at AMU/APUS for the role it has played in my growth over the years. In addition, I would like to thank the countless friends and mentors not mentioned in this acknowledgment. Each of you has been vital to helping me get to this point —THANK YOU!

ABSTRACT OF THE THESIS

COGNITIVE AND INFORMATION WARFARE IN THE NEW STRATEGIC REALITY: EXAMINING THE NEED FOR UPGRADING U.S. OFFENSIVE AND DEFENSIVE CAPABILITIES AGAINST MALIGN ADVERSARIES

by

Sam Kessler

American Public University System, April 2024

Charles Town, West Virginia

Dr. Al Lewis, Thesis Professor

The international system is becoming more volatile and multi-polar and these changes greatly impact the strategic reality of the United States and its leadership. The globalization era was a prosperous era, but it also enabled state and non-state actors to rise in strength and capabilities during this period. For the first time since the end of the Cold War we are experiencing the rise of both old and new rivals compete for influence in this international system. As a result, the U.S. has experienced an increase in malign influence attacks consisting of cognitive and information operations by adversaries like China and Russia. However, the U.S. needs to address these problems and improve its offense and defense capabilities in dealing with cognitive and information operations. This qualitative analysis paper will address non-kinetic warfare doctrines and strategies used by U.S. adversaries and apply them into two case studies on China and Russia who are predominant players in this area of warfare. Lastly, this paper will assess current weaknesses addressed in a report about the DoD Military Information Support Operations (MISO) offensive and defensive capabilities in cognitive and information warfare and discuss suggestions for improving and adapting them to deal with rising threats.

TABLE OF CONTENTS

CHAPTER	PAGE
I. INTRODUCTION.....	1
II. LITERATURE REVIEW.....	13
Understanding U.S. Strategic Reality: Evolving Multi-Polar System.....	13
Debate on Cognitive vs. Human Domain in Multi-domain Warfare.....	19
Cognitive and Information Operations: Improving Offensive and Defensive Capabilities.....	23
III. RESEARCH METHODOLOGY.....	28
Research Design.....	30
Research Methods.....	33
Data Collection Methods.....	33
Data Analysis Process – Qualitative Analysis.....	34
Research Limitations.....	51
Summary.....	51
IV. FINDINGS & ANALYSIS.....	53
Societal Spheres of Influence Impacted by Malign Adversaries.....	53
Operations Leading to Societal Disruption, Volatility, and Failure.	61
China Case Study.....	62
Russia Case Study.....	64
U.S. Offense and Defense Capabilities in Cognitive and Information Operations...	66
Assessing MISO’S Problems and Areas for Improvement.....	66
MISO: State of Operational Decline.....	67
MISO: Recommendations for Improving Offense and Defense Capabilities.....	68
V. CONCLUSION.....	70
VI. AREAS FOR FUTURE RESEARCH.....	73
VII. LIST OF REFERENCES.....	74

LIST OF TABLES

TABLE	PAGE
1. TABLE: 1.....	39
2. TABLE: 2.1.....	40
3. TABLE: 2.2	41
4. TABLE: 3	42
5. TABLE: 4	43
6. TABLE: 5	44
7. TABLE: 6	47
8. TABLE: 7.1	48
9. TABLE: 7.2	49
10. TABLE: 8	50

LIST OF FIGURES

TABLE	PAGE
1. FIGURE: 1.....	38
2. FIGURE: 2.....	46

CHAPTER 1: INTRODUCTION

Using false information to gain an advantage over one's opponent is nothing new in the history of strategy. Churchill, for example, is said to have told Stalin, "In wartime, the truth was so precious that it should always be attended by a bodyguard of lies."

—David Pappalardo (War on the Rocks 2022).

OVERVIEW

The end of the Cold War enabled the U.S. to have a newfound status within the international system as the sole remaining superpower in an era where globalization became part of its policy of preponderance. This new era generated a global system of interconnectedness and interdependence between societies that became streamlined at unprecedented levels in history. The result of these new changes in the international system has been discussed and examined thoroughly by scholars and practitioners since the end of the Cold War regarding the U.S. ability to manage its status and ongoing role as the leader of a world order that followed the demise of the former Soviet Union. Despite the changing circumstances, the U.S. continued to preserve the grand strategy it formulated during the Cold War and utilized it for the new globalization era that followed. This approach was articulated by Christopher Layne in his 1997 paper, "From Preponderance to Offshore Balancing, America's Future Grand Strategy" where he described how the U.S. was applying the strategy in the international system that was evolving when he said that:

The key elements of this strategy are creation and maintenance of a U.S.-led world order based on preeminent U.S. political, military, and economic power, and on American values; maximization of U.S. control over the international system by preventing the emergence of rival great powers in Europe and East Asia; and maintenance of economic interdependence as a vital U.S. security interest. The logic of the strategy is that interdependence is the paramount

interest the strategy promotes; instability is the threat to interdependence; and extended deterrence is the means by which the strategy deals with this threat (Layne 1997, 88).

Three decades later, the U.S. finds itself in a different situation and scenario as it manages its leadership status within an international system that is once again changing and evolving with increased volatility and competition from other state and non-state actors. In fact, a rising China and a resurgent Russia on the world stage, along with the increasing threat of larger conflicts occurring in Eastern Europe, the Middle East, the Indo-Pacific, and other areas around the world have illustrated greater volatility, competition, and multipolarity in the international system (Kessler 2022). This can significantly impact the future of American great power projection. Although, the U.S. is not currently engaged in a full-scale direct kinetic conflict with an adversarial foreign malign actor, it remains active in dealing with its non-kinetic threats. In addition, it is also managing these threats within an international system where the world's militaries are increasing and cultivating their capabilities to integrate information and kinetic operations at the multidomain level (Cruickshank, Windmueller, and Benigni 2023).

Brose reinforces this point when he mentions that U.S. adversaries are already utilizing non-kinetic warfare as they are catching up very quickly and “are far more provocative, organized, funded, and technologically capable than what current American forces have addressed and learned from for the past 30 years” (Brose 2020, 29). However, it is important to note the complexities of modern warfare where operations tend to be utilized for targeted or specified purposes, which means there may be a blend of domains involved, whether kinetic or non-kinetic based. Pomerleau mentions the differences between kinetic and non-kinetic as, “in U.S. military parlance,

the term ‘kinetic’ generally refers to missiles or other traditional types of weapon systems that physically engage targets, whereas non-kinetic tools can include cyber, electronic warfare and other means of attack” (Pomerleau 2023, n.p.). This also includes using non-kinetic capabilities that pertain to both cognitive and information operations at both the offensive and defensive realms. In addition, this paper will focus primarily on the use of cognitive and information operations in the non-kinetic battlefield that consists of both the foreign and domestic domains and the impacts on societal spheres of influence.

By focusing on these issues, the paper will be helpful since the increased volatility that is impacting the state of the current U.S. strategic reality in the international system raises serious questions regarding the status of offensive and defensive functions relating to cognitive and information operations. It is both a timely and important area of focus since this is an ongoing issue and concern being raised by both the military and civilian sectors within the U.S. national security and intelligence communities. After all, the level of offensive and defensive capabilities that are applied can have a significant impact on the U.S.’s ability to combat the operational efforts of malign adversarial actors (Dundon 2021). This research paper will explore these concepts and discuss the growing need for improving and adapting offensive and defensive capabilities pertaining to cognitive and information operations. In addition, it will discuss how these realities impact or impair societal spheres of influence since the domestic domain can also be incorporated as a non-kinetic battlefield as well. An exploration of ways to tackle these processes and recommendations for improving the effectiveness of countering foreign adversarial malign influence in relationship to

cognitive and information operations will follow.

Definitions

The following definitions and descriptions will help provide the reader with an understanding and ability to differentiate between cognitive warfare, cognitive operations, information warfare, and information operations. This will help the reader to quickly ascertain these concepts and definitions when applied in various sections throughout this paper.

Cognitive Warfare:

There are two useful definitions of cognitive warfare that are effective and influential for understanding the big picture purposes of this domain. The first is that cognitive warfare “is a strategy that focuses on altering how a target population thinks and through that how it acts” (Backes and Swab 2019, 8). The second definition adds that cognitive warfare is “the weaponization of public opinion, by an external entity, for the purpose of influencing public and/or government policy or for the purpose of destabilizing governmental actions and/or institutions” (Bernal et al. 2020, 10). The author chose to combine these two definitions to strengthen the clarity and focus for this paper with the following,

Cognitive warfare is a strategy that focuses on altering how a target population thinks and through that how it acts. It particularly deals with the weaponization of public opinion, by an external entity, for the purpose of influencing public and/or government policy or for the purpose of destabilizing governmental actions and/or institutions (Kessler 2024).

Unlike conventional warfare, which is kinetic in nature, cognitive warfare is not considered to be physical but still pertains to Clausewitz’s definition of war as “an act of force to compel our enemy to do our will” (Clausewitz 1989, 75-89). This relates to

the strategy of cognitive warfare, which seeks to create a situation or scenario that influences an enemy to damage or destroy themselves from within to the point that cripples their ability to resist, deter, or deflect the goals of their adversary (Bernal et al., 2020). The successful implementation of this strategy would either make kinetic warfare easier to apply in the adversary's favor or render it unnecessary if desirable results created that outcome. Either way, the results could lead to the degradation of rational thinking that can cause systemic vulnerabilities to be further exploited. This is especially impactful when considering how this approach can be applied to societal spheres of influence if targeted and exploited by a malign actor or foreign adversary through its cognitive or information operation.

Cognitive Operations:

Danyk and Briggs (2023) provide a detailed description of cognitive operations that adds to the discussion regarding the implementation of cognitive warfare. They described cognitive operations “as the coordinated goal (target), scope, location, and time parallel and/or consequent actions, which support influence on the highest level of human thought, outlook, values, knowledge, and interests. Cognitive operations affect people’s perception of reality and decision-making, guiding groups of people and targeted audiences towards conditions desired by a geopolitical adversary” (Danyk and Briggs 2023, 36). In addition, it was also explained that cognitive operations can also be utilized as tools for preventive actions that can decrease the risks and threats of conventional or kinetic wars. However, their description also described cognitive operations as being digital tools for expansion or colonization via transformations of outlook, values, and interests of targeted groups. This approach would not only impact

the stability of societal spheres of influence and the people involved, but also impair its ability to properly defend itself as well.

Their description also adds that cognitive operations are very specific, which means they are very deliberate, and that influence or expansion efforts are not spontaneous or self-regulating (Danyk and Briggs 2023). Another way to imply this is to make the statement that nothing happens in a vacuum, particularly when cognitive and information warfare is being applied to the scenario. They also mentioned that cognitive operations are focused on managing people's worldviews, interests, and values that pertain to non-physical colonization of societies. In the digital realm, they mention that modern information and digital technologies can be fostered with the use of data harvesting, artificial intelligence (A.I.), social media, and other online data sources can be utilized for these purposes (Danyk and Briggs 2023).

In addition, other examples can include cybertechnologies, algorithms, and automated software such as bots mimicking real people which has increased the potential for spreading "disinformation, misinformation, conspiracy theories, hate speech and propaganda on the part of a wide array of actors" (Miller 2023). These types of operations can cause great harm to a society if they succeed at disrupting and altering rational thought and understanding of realities by citizens in both the public and private sectors. In fact, such cognitive operations could be used strategically to disrupt the ability to respond to immediate and distant threats as well.

Information Warfare:

Information warfare is related to cognitive warfare since they tend to collaborate collectively in the operational realm. However, it is distinctive when compared to the

role and way of thinking in cognitive warfare. In short, information warfare is mainly centered on the control of the flow and access to information (Bernal et al. 2020).

Bernal et al. reiterate this point when they mentioned that the sharper delineation between information warfare and cognitive warfare “is that information warfare seeks to control pure information in all forms and cognitive warfare seeks to control how individuals and populations react to presented information” (Bernal et al. 2020, 8-9).

This is why it will be helpful when examining how and why societal spheres of influence are impacted and how U.S. offense and defense operations in the cognitive and information domain can be improved.

Information Operations:

Information operations are primarily the capabilities for implementing information warfare as well as supporting cognitive warfare strategies. They include electronic warfare, computer network operations, psychological operations (PsyOps), military deception, and operational security (Bernal et al., 2020). An alternative and more simplistic description of information operations is described by Kuehl as being “actions taken to affect adversary information and information systems while defending one’s own information and information systems” (Kuehl 2002, 36). This adds to the discussion of adapting and improving defensive and offensive capabilities as well as how societies can be influenced by information operations since it is a targeted and heavily focused process that serves a specific purpose.

Purpose Statement

The author assumes that U.S. offensive and defensive operational capabilities in the cognitive and information domain will require continuous updates to reflect the changing and evolving strategic realities in a more volatile international system. These

types of processes are usually under constant evolution in an operational environment that is constantly changing in real-time. Arguments illustrate various opinions on this matter, but strong research indicates that there is indeed a need for upgrading U.S. offensive and defensive capabilities regarding cognitive and information operations. The aim of this thesis paper will assess and examine this research and offer insights pertaining to recommendations that will also offer improved understanding of these ongoing issues and concerns. It will also seek to answer the questions that deal with the discussion on improving U.S. offense and defense capabilities. In addition, this paper will also address how cognitive and information operations by hostile foreign malign adversaries can be used to impact and impair societal spheres of influence since it can be utilized as a domestic battlefield. This is important for addressing since the health status of societal spheres of influence can determine the ability for it to survive and thrive after a targeted attack.

Research Questions, Hypothesis, and Variables

The main research question for this thesis asks how the societal spheres of influence are impacted by cognitive and information operations by hostile foreign malign adversaries and what can be done to improve U.S. offensive and defensive capabilities in a more volatile international system. This is followed by sub-research questions to help build onto the primary research question as it will help shed light on the focus and purpose of this paper on cognitive and information operations. Sub-research questions will be asking for further verification regarding the identification of the societal spheres of influence, cognitive and information operations, current offensive and defensive capabilities, and ways to improve this process in a more volatile

international system. The following defines the specifics regarding the main research question and the additional research questions that illustrate the focus of this paper and its representation of this thesis's hypothesis:

Main Research Question:

- How are societal spheres of influence impacted by cognitive and information operations by hostile foreign malign adversaries and what can be done to improve U.S. offensive and defensive capabilities in a more volatile international system?

Additional Research Question #1:

- What are the societal spheres of influence and how can they be manipulated and influenced in the non-kinetic battlefield?

Additional Research Question #2:

- What are cognitive and information operations and how are they used for influencing and manipulating at the kinetic, non-kinetic, and multi-domain level?

Additional Research Question #3:

- What recent and previous approaches have been applied by the U.S. that focused on strengthening and adapting its offensive and defensive capabilities that pertain to countering cognitive and information operations by its foreign malign adversaries?

Additional Research Question #4:

- How should the U.S. improve and adapt its offensive and defensive capabilities in its cognitive and information operations in an international system where there is greater volatility than previously?

Hypothesis

- Increased volatility by hostile foreign malign adversaries in the international system requires the U.S. to strengthen and adapt its offensive and defensive capabilities to combat the threat.

Independent and Dependent Variables

- **Independent Variables:** Spheres of influence impacted by cognitive influence and information operations by foreign malign adversaries.
- **Dependent Variables:** Offensive and defensive capabilities currently being used and considered for countering adversarial malign cognitive influence and information operations.

Research Method

The research method for this thesis paper will utilize qualitative analysis that incorporates the grounded theory regarding collection and analysis. This will be helpful as it enables cutoff points for the author in the research and analysis portion of this paper. In addition, this thesis will utilize two additional theories that are relevant to the overall focus of this research paper: the realist theory and rational choice theory. The author will take realist and rationalist approaches to assessing and examining the material dealing with this topic. The rationale is that it is assumed that actors involved on both ends of the spectrum are also employing a realist and rationalist mindset

approach in their decisions, policies, actions, and desired outcomes. In other words, it is assumed that all players involved are employing both a strategic and tactical approach to cognitive and information operations.

Limitations

Limitations in this qualitative analysis will deal with the realist, rational, and U.S.-centric nature of this paper since its goals are to collect and analyze information that can improve the U.S. intelligence and national security communities' ability to improve offensive and defensive cognitive and information operations. Also, the themes discussed in this paper are still considered emerging and ongoing with the evolving nature of the geopolitical threat landscape occurring in real-time. This means there is a cutoff of information collection for analysis in this thesis. Lastly, the information collected for this qualitative analysis will be based on unclassified open-source material rather than relying on classified sources.

Summary

Subsequent chapters in this thesis will discuss in greater detail the key themes and points addressed in the purpose and goals of this research paper titled, "Cognitive and Information Warfare in the New Strategic Reality: Examining the Need for Upgrading U.S. Offensive and Defensive Capabilities Against Malign Adversaries". Chapter 2 will serve as the literature review section of this paper where a review of pertinent literature on key themes related to this thesis will be discussed. This section will help the reader gain helpful insights into the subject matter as well being able to put into context in the subsequent sections of this research paper.

Chapter 3 will discuss the research methodology of this paper as it will delve

into greater detail the research design and methods that were used to make this thesis an effective qualitative analysis that utilized grounded theory, realist theory, and rational choice theory. The 4th chapter will incorporate the research findings and analysis of this paper as it will utilize the hypothesis and research questions for the areas being examined and discussed. Chapter 5 will be the conclusion of this paper where it will summarize what has been discussed and examined by the author. In addition, it will assess future areas of research that may help practitioners and scholars in their own research, examinations, and inquiries whether for academic or professional purposes.

CHAPTER 2: LITERATURE REVIEW

Overview

This literature review will provide a discussion on three themes that pertain to the focus of this thesis. It begins with discussing U.S. strategic reality in an evolving multi-polar system, which discusses arguments and interpretations on the evolving state of the international system and the future of American preponderance. The second theme deals with arguments pertaining to the cognitive and human domains in multidomain warfare in which there is a discussion on societal spheres of influence. The third theme deals with arguments that contribute to the discussion on improving U.S. offensive and defensive capabilities in cognitive and information operations. It is important to note that the author's intention is to build onto each theme to help the reader understand the importance of the key points being made, as well as viewing the evolution of the arguments being discussed within a narrative format. In addition, the themes in this literature review should also help answer the research questions or at least contribute to having a firm foundation for them.

Understanding U.S. Strategic Reality: Evolving Multi-polar System

The first theme of this literature review will start with reviewing the concepts of understanding U.S. strategic reality in an international system that is showing signs of evolving into a multi-polar world. It is necessary to address these themes since cognitive and information operations are increasing by U.S. adversarial and hostile actors in recent years (MacDonald and Ratcliffe 2023). Both cognitive and information operations have plenty of literature over the years and have been part of multidomain operations throughout the U.S. national security and intelligence communities (Nettis 2020). However, the issue of addressing it in terms of a new U.S. strategic reality and evolving multi-polar international system is relatively recent in what

will be addressed as being a post-Global War on Terror (or Post-GWOT) era. Discussing it in this section as part of the theme will apply to the concepts that help describe and define the period.

Understanding this period is essential since cognitive and information operations in a more volatile international system are occurring and can impact how the U.S. maneuvers itself. In addition, it will also have a great impact on the way the U.S. manages its power projection in a competitive environment filled with state and non-state actors with greater disruption skills and capabilities than in previous eras. MacDonald and Ratcliffe reinforce this point when they mention, “Cognitive warfare operations are growing rapidly in quantity, range, precision, and effectiveness, increasing their potential to achieve strategic success. As these capabilities grow, operations are increasingly able to evolve into complex attacks, with synchronized actions across domains achieving nonlinear effects” (MacDonald and Ratcliffe 2023, n.p.). Lastly, today’s wars are fought in both the kinetic and non-kinetic battlefields, which means that “strategy is about perception, and cognitive warfare in information spaces is on full display with wars between Ukraine and Russia and Israel and Hamas” (Jensen and Ramjee 2023, n.p.). It also occurs in other areas in the non-kinetic battlefield, which will also be discussed in subsequent themes in this literature review.

Globalization Causing the Emergence of a New Multi-polar System

The first section of this theme begins with a discussion on the current state of the international system and its linkages to the last three decades of globalization and interconnectedness that came to fruition after the Cold War ended in the early 1990s. Discussing it is important given the level of impact it has on the world and how its interconnected nature illustrates how hard it is for international trends not to occur in a vacuum. Globalization is

essential for assessing current and future trends in the international system during this time since it was considered a period that enabled nearly all countries throughout the world to become richer than in previous decades. Dr. Douglas Irwin reiterates this when he mentioned how most countries are much better off now than three or four decades ago when the globalization era began (Irwin 2022, n.p.). He also adds that globalization cannot be described as a zero-sum game where the gains for some countries are at the expense of others because the “vast economic gains made by poor countries in the past few decades have not come at the expense of advanced countries” (Irwin 2022, n.p.).

However, the mid to late 2000s started showing signs of the international system’s evolution, and the outlook’s trends and catalysts were beginning to illustrate growing uncertainties and disparities. In fact, it was exhibited in the 2008 Global Trends 2025 report by the U.S. National Intelligence Council, which noticed several major changes from economies and wealth transferring, increased power projection of state and non-state actors like China, India, businesses, religious organizations, and criminal networks, along with greater competition for resources, technology, and military capabilities (Fingar 2008). The document warned that the formation of a new multi-polar system was inevitable but with great uncertainties of outcome. In addition, it mentioned that the transition would be fraught with risks and that “strategic rivalries are most likely to revolve around trade, investments, and technological innovation acquisition, but we cannot rule out a 19th century-like scenario of arms races, territorial expansion, and military rivalries” (Fingar 2008, vi). It was an indication that this era was generating an environment for greater friction and competition between old and new rivalries that was becoming more realistic and troublesome in the U.S.-led order where it had been previously marginalized after the Cold War ended.

The Primakov Doctrine: Long-Term Russia and China Multi-polar Initiative

The next section of this theme deals with the discussion regarding the influence of a strategic partnership between Russia and China that is impacting the current state of the international system, which is becoming more multi-polar. It illustrates how realism and rationalism can be incorporated by state actors in the context of utilizing power projection initiatives to impact long-term geopolitical security trends, such as influencing conditions that promote the growth of a multi-polar system. The end of the Cold War witnessed the thaw in Russian and Chinese relations that have since deepened within the last three decades. It has particularly been greatly enhanced recently since the current Russian war in Ukraine foreshadowed the “No Limits” partnership forged by Russian President Vladimir Putin and Chinese President Xi Jinping, illustrating deeper security, defense, and economic ties between Moscow and Beijing (Gabuev 2023). A long-term and evolving strategic partnership between China and Russia has been occurring since the mid-1990s and has been illustrated through a series of friendship and good neighbor agreements (Cohen 2001).

The strategic partnership between Moscow and Beijing is also related to what has been called the Primakov doctrine, which was created by former Russian foreign minister Yevgeny Primakov after the Soviet Union collapsed, which ended the Cold War (Rumer 2019). However, this change in geopolitical dynamics continued to show the shared Russian and Chinese concern for the new international system developing after the Cold War which became unipolar and led by the United States. The Primakov doctrine was designed as a long-term strategy to challenge and dilute U.S. power and leadership role in global security as well as “preventing a monopolar world dominated by a single superpower” (Cohen 1997, 3). A Moscow and Beijing partnership evolved out of this doctrine and enabled the possibility of welcoming other powers like Iran,

India, and France into this endeavor.

Although, it remains a strategic partnership, China is considered the senior partner given its larger strength and position as a global power in the international system. In recent times, the Primakov doctrine has been considered the influential mechanism that promotes the development of a new trilateral alliance between Russia, China, and India, also known as RIC, which would emphasize a multi-polar international system and seek to provide a united front to resist the U.S. role as the world's sole superpower (Shabbir 2023). It illustrates that the Primakov doctrine remains not only influential in Russia's foreign policy focus but also in other nations looking to project their own power in this evolving international system that has become more volatile. In addition, the manner in which nations react and respond to Russia's invasion of Ukraine and a potential invasion of Taiwan by the People's Republic of China (PRC) will be additional indicators of this as well.

U.S. Strategic Reality in the Post Global War on Terror Era (Post-GWOT)

The state of the U.S. Global War on Terror (GWOT) and an evolving concept dealing with a post-GWOT era will be discussed in this section. It will shed light on the new and evolving threats dealing with larger and more sophisticated adversarial actors becoming a more potent focus in U.S. strategic reality. The GWOT era in two decades had ranged from military campaigns in Iraq, Afghanistan, and Syria, as well to combatting and countering terrorist networks on multiple continents, and counterterrorism-based operations that are still occurring in numerous countries (Georgetown Bridge Team 2023). However, the focus of the GWOT is no longer considered the predominant focus of U.S. national security policy since the international system has evolved greatly since the September 11th 2001 terrorist attacks. Although, the Biden administration did illustrate in their remarks about the 2021 end-withdrawal of U.S. troops in

Afghanistan by keeping options open as a continued policy to combat terrorist networks without having American boots on the ground. In short, it emphasized increasing over-the-horizon capabilities that utilize drone strikes and the use of special operations forces to combat and counter global threats from terrorist networks (White House 2021).

Another concept that relates to the post-GWOT era argument pertains to the concept of increased proxy warfare shaping the future of twenty-first century conflicts. The concept of proxy warfare in a multi-polar post-GWOT era is different from the Cold War era since that was a bipolar international system. A multi-polar system with increased global proxy warfare by numerous state and non-state actors is a very different game and playbook that no longer includes just Washington and Moscow setting the rules (Rondeaux and Sterman 2019). In addition, a bipolar system enabled two main players, the U.S. and the former Soviet Union, during the Cold War to play by a set of rules and standards that created the nature of the playing field, which, in a sense, showed predictability in outcomes.

However, the evolving multi-polar system deals with a wide range of actors that sponsor and support proxy forces and operations, such as states, non-state actors, corporations, mercenaries, and militias that are “changing the way wars are fought and won” (Rondeaux and Sterman 2019, 3). In addition, proxy warfare is either centered on conventional or irregular forces that go outside the traditional actor’s constitutional mandates (2019, 3). A good example of this could be the Iranian government’s proxy network of Shia paramilitary groups that they funded and trained throughout the Middle East via Lebanon, Iraq, Yemen, and Syria, which also enabled them plausible deniability (Thomas 2020). Examples like this reinforce the point that proxy warfare has become more attractive and lucrative in an international system that is more volatile and possesses greater competitive actors than in previous eras. Lastly, this is a type of

warfare where cognitive and information operations would play an influential role in the theatre as well. After all, the U.S. may be tempted to apply more non-military approaches rather than the direct use of force to prevent the overstretch of assets resulting from a potential kinetic conflict (Allison 2020).

Conclusion

The different concepts and explanations discussed in this theme captured the various arguments and perspectives in understanding the U.S. strategic reality in an international system that is becoming more volatile and multi-polar. They illustrate the various viewpoints in understanding why the international system has changed and evolved. In addition, these concepts also show how cognitive and information operations may be attractive options for adversarial actors. While there are several concepts and explanations, each of these is related and helps the reader understand how the evolution of globalization, Russia's Primakov doctrine, the China-Russia strategic partnership, and the post-GWOT era can play a role in impacting the current state of U.S. strategic reality and the international system that is becoming more volatile and multi-polar.

Debate on Cognitive vs Human Domain in Multi-domain Warfare

Another important theme that this literature review will address is the debate that deals with placing emphasis on the cognitive versus the human domain of warfare. Both tend to work collectively and with similar objectives in operations and strategy. While the cognitive domain is emphasized in this paper, it is important to note that the human domain plays a significant role in conjunction with it. In fact, the human domain also plays a role in its relationship with the various spheres of societal influence that can be disrupted by a malign adversary. Some of the arguments about this theme have discussed both the relevance and the differences between

cognitive and human domain warfare. These arguments range from the cognitive domain being too limited in focus as part of the arsenal of offense and defense capabilities, while others consider the human domain too broadly oriented. The reality is both are multi-domain-based forms of warfare that continue to require multidisciplinary mindsets, which is essential to emphasize since adversaries like China and Russia are performing these similar approaches (Branch et al. 2021).

Human and Cognitive Domains

The relationship between the human and cognitive domains of warfare will be examined in this section. Professionals and academics in the military and intelligence sectors have debated the use of terms. Hofstetter and Jossen utilized general model theory to determine whether there was a requirement for an official cognitive domain and concluded that it was not needed. They looked at the value of cognitive domain between the variables of actual warfare and ideal warfare and determined it was too strongly intertwined with other domains that it could not be independent. In addition, they viewed the differences between the domains as either being physical or meta-physical as well. They emphasized these points when they mentioned that applying both General Model Theory and NATO's definition of Multi-Domain Operation (MDO) showed no requirement for a cognitive domain since MDO as a model was intended for only simplifying the work of military planners and commanders (Hofstetter and Jossen 2023, n.p.). In addition, they also mentioned that while they realized that cognitive warfare is important, it is the reality that cognitive effects in warfare are less related and more different in relationship to the specific domain they occur in (Hofstetter and Jossen 2023, n.p.).

Another argument discusses the human domain of warfare being larger and more dynamic in coverage than cognitive warfare. In fact, supporters of this argument believe

cognitive warfare is limited, restricted in use, and is more of a single tool in a vast arsenal, while the human domain is the one defining individuals and the structures of our societies such as, “Political science, history, geography, biology, cognitive science, business studies, medicine and health, psychology, demography, economics, environmental studies, information sciences, international studies, law, linguistics, management, media studies, philosophy, voting systems, public administration, international politics, international relations, religious studies, education, sociology, arts and culture ...” (NATO Symposium 2021, 3-2). In addition, Heather Gregg built on previous definitions of the human domain by U.S. Southern Command (USSOCOM) and defined it as the following: “The human domain is comprised of humans—including humans as physical beings, human thought, emotions, and human action—and what they create, such as groups, infrastructure, art and so on. In other words, the human domain is what humans are, what they think, how they act, and what they create” (Gregg 2016, 94).

Gregg’s definition resonates with the concept in this thesis that deals with societal spheres of influence, which are considered a part of the human domain of warfare. In addition, it relates to the type of human domain operations that are utilized by U.S. adversaries like China and Russia. In fact, both adversaries deal with operations and doctrines that relate to the human domain that are also cognitive domain related. It is imperative to address them since they also correlate with the social sciences and humanities, which also are elements that pertain to societal spheres of influence. However, it is also believed that they belong in the multi-domain category since they can be on equal footing with the hard sciences that relate to the other domains of warfare (NATO symposium 2021, 3-3). Gregg addresses the need for a human domain for the armed forces by incorporating four competencies that are broad and necessary to understand and influence it within the following areas. They are language and cultural analytics, which enables

the ability to analyze culture within an operation; communication skills; intelligence capabilities; skills preparation for military interagency, whole of government, and whole of nation (Gregg 2016, 93).

In addition, the human domain as a multi-domain capability is considered an element that is hard for the U.S. military and interagency to compete in comparison to the other physical and kinetic domains like air, land, sea, cyber, and space. Branch, Cardon et al mention that the problem is rooted in institutional culture and the way DoD trains and prepares for multi-domain warfare (Branch, Cardon et al. 2021). They reiterate that the human domain surpasses the academic realm as it is where great power competition is playing out before it becomes a major kinetic conflict. However, they also add that the defense enterprise is not only unprepared in the human domain for a large-scale kinetic event but also for conventional capabilities in response to adversary operations in the information environment (Branch, Cardon et al. 2021). They also mention that authoritarian adversaries operate freely within the human domain which means the U.S. needs to embrace a new information paradigm and develop capabilities for improving agility and tactics when dealing with uncertain scenarios (Branch, Cardon et al. 2021).

Lastly, it is important to note that the Chinese People's Liberation Army (PLA) utilizes a cognitive domain approach but still takes a multi-domain and multi-dimensional approach to its understanding by incorporating both human and cognitive elements of thinking, perception, psychology, and societal spheres of influence (McClenon 2023). In addition, McClenon discusses this concept of strengthening the cognitive domain as well as applying the human domain for the United States when he mentioned that the Department of Defense began with the concept of a cognitive warfare domain but it is now behind the curve and will need to go to greater lengths at restrengthening that skill where one must understand "the psychological

weaknesses, patterns, behavior, and motivations of the target population in order to effectively disrupt decision-making and other activities in one's own favor, or at least against the target's interests (McClenon 2023, n.p.).

Conclusion

It was valuable to address the similarities and differences between the cognitive and human domains as well as looking at their multi-domain elements in this theme. In addition, it was helpful to examine the various ways it has been interpreted for operational implementation by the U.S. and its adversaries like China and Russia. While this thesis emphasizes the cognitive domain, it also views it from the human domain as well. Doing this makes it possible to assess the various types of operations where the hard sciences and kinetic domains must emphasize human elements that are illustrated in societal spheres of influence that are also of a non-kinetic nature. Such societal spheres of influence are vast and deal with the social sciences and humanities, which is why it is considered difficult to be a primary focus. However, the human domain is often utilized for correlating with the cognitive domain and other domains as a multi-domain, multi-disciplinary, and multi-dimensional elements, which is an area that the debate also addressed in terms of future improvement, training, and better preparedness when dealing with malign adversaries in the cognitive and non-kinetic battlefield.

Cognitive and Information Operations:

Improving Offensive and Defensive Capabilities

Creating the need for the U.S. to improve its offensive and defensive capabilities for cognitive and information operations will be discussed in this theme. The popular belief held by practitioners and scholars in this debate agrees with the need to be better prepared in this warfare domain. However, the literature that offers recommendations is still considered to be limited.

More is still needed to offer recommendations on ways the U.S. military can “defend against perceptual manipulation” and countering weaponized information, as this would greatly impact the liberal belief system of openness and free press (Hall 2023, 76-77). A big concern that Joseph Nye mentions is the inability to achieve credible information in a censorship environment, as government-subsidized information is rarely perceived as being credible or reliable by the masses (Nye 2013). The dilemma this creates is the openness of the system being both a strength and vulnerability for a society that values free speech while seeking to protect its society and preventing the perceptual manipulation of its spheres of influence on the domestic non-kinetic battlefield.

Institutional Culture and Training

The previous theme referenced the need to improve the way cognitive and information operations professionals are trained and the institutional culture in which they operate to be more effective (Branch, Cardon et al. 2021). Pappalardo mentions that it’s important for cognitive warriors to be more mindful of their own individual, collective cognitive functions, and it requires one to possess the knowledge and ability to identify their cognitive biases that can precondition mental patterns (Pappalardo 2022). However, he also adds that groupthink mentality tends to be very common in bureaucracies, which can greatly impair the ability to properly read situations, threats, and adversaries properly. After all, bad analyses and interpretations can mean lives and disastrous outcomes.

Papalardo also emphasized the importance of not being over-reliant on the utilization and focus of technology and that the military needs to find a fine balance between human and system integration to retain clarity in a complex wartime environment. He adds that it is essential to emancipate oneself from utopian ideals of thinking that only technology will help a person

understand the battlefield. While he realizes the value of incorporating technology into the battlefield, he also understands that it can also illustrate cognitive dissonance, as well as producing opposite and unfavorable results due to things like algorithms and database having unrecognized biases (Pappalardo 2022, n.p.).

Colonel Hall adds to this discussion when mentioning the need for the U.S. military to codify a cognitive warfighting domain to help improve institutional culture, training, and being better prepared from malign adversarial non-kinetic threats and attacks. Hall discusses that information experts tend to advocate the U.S. Congress to enact laws that don't leverage military capabilities to combat and counter cognitive and information operations. However, he suggests that they need to incorporate this to improve military culture and training by having the Joint Staff formalize the cognitive warfighting domain since Joint Publication 3-13, Information Operations does not discuss how to shape target audience perceptions for desired strategic effects. Hall also mentions that formalizing it would provide the military enterprise with the ability to prevail on the cognitive battlefield by reflagging "U.S. Cyber Command and consolidating cyber, electronic warfare, military information support operations, civil affairs and all other functions into a primary U.S. Cognitive Dominance Command" (Hall 2023, 84-85). This idea would not replace cyber but to restructure the entire information spectrum as the joint warfighting integrator for strategic cognitive competition with adversaries.

Focusing on Human Will in the Cognitive Battlefield

Another argument regarding the need to improve offensive and defensive capabilities deals with the human emphasis in responding to or implementing cognitive attacks on societies. Adversary malign actors apply methods that exploit cognitive gaps where malignant information thrives and help them manipulate societies to reach their strategic cognitive aims and objectives

(Hall 2023). Closing the exploitable cognitive gaps has been discussed as an approach to counter propaganda by malign actors since the strategy can be mapped out by professionals and practitioners seeking to counter it. After all, strong emotions are determined by the individual and their reaction to the manipulated narratives and propaganda. Hall emphasizes the importance of doing more to improve the understanding of the framework that was created by the malign actor via dissonance reduction manipulation that can improve our understanding “of how entire societies may be influenced to commit self-destructive behaviors” (Hall 2023).

Maneuver warfare has also been discussed to improve offensive and defensive capabilities in cognitive and information operations in the human domain area. The argument is aimed at countering and combatting cognitive and information operations by “seeking to shatter the enemy’s cohesion and create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. To manufacture this situation, maneuver warfare synchronizes physical maneuver, fires, and mass across multiple domains while exploiting tempo” (Marine Corps Warfighting 1997, 71-73). In addition, this is a Marine Corps concept that also applies to cognitive and information warfare as it seeks to create the conditions first to destroy the enemy’s ability to function on the battlefield. In this instance, certain cognitive elements would have to be in place prior to or immediately to disrupt enemy operations. MacDonald and Ratcliffe mention that the U.S. approach should emphasize U.S. values and methods that introduce both truthful and impactful narratives when concentrating on certain targets, as it will help preserve legitimacy in the long run within the global information space (MacDonald and Ratcliffe 2023).

Conclusion

Important areas relating to the debate on improving the offensive and defensive capabilities in the cognitive and information operational domain were addressed in this theme. It

addressed areas that dealt with institutional issues of limitations regarding training and culture as well as preparing multidomain thinkers. Greater emphasis can lead toward countering and combatting malign cognitive attacks with a more advanced understanding of how it was implemented. In addition, a human-oriented approach was discussed with a healthy balance in technology use while not being overly reliant on big data, which can also have its biases and limitations. Lastly, it was also discussed that the U.S. needed to take a more proactive approach to countering a malign cognitive attack with a strategy that rips the enemy's battle edge early on while incorporating elements of U.S. values, narratives, and truths to help build long term legitimacy and stability.

CHAPTER 3: RESEARCH METHODOLOGY

Overview

This qualitative analysis of the impact of cognitive influence and information operations on societal spheres of influence requires a design and methods process that can properly handle the open-ended and never-ending nature of this research project. It also enables the author to examine the material with a fresh lens and the ability to piece it together in a manner that offers a big picture understanding for the reader to understand. The incorporation of grounded theory in this project as a method of collecting and analyzing data until research saturation is achieved will be helpful for ensuring a proper cut-off point (Lumivero 2023). In addition, this qualitative study also utilizes both the realist and rational choice theories, which will be discussed later in the research design portion of this section. Both theories are based on the realism and rationalism of state actors, which pertain to the reasons why adversarial and hostile foreign actors may implement cognitive influence and information operations. This reinforces the concept that a realist cognitive war is about removal of choice to the people with a targeted bias that may weaken spheres of influence within American society and the national security realm. Lastly, the author of this paper assumes that the decisions by actors to implement cognitive and information operations are based on rationalist and realist thinking since they tend to be processes that are targeted and focused oriented.

The qualitative nature of this research project, in addition to the utilization of the grounded, realist, and rational choice theories in this analytical research has made it significantly easier to determine appropriate and relevant questions for this project. These questions under the qualitative process will enable saturation with relevant themes and insights in the analytical process. This will be achievable since the emphasis deals with how malign actors via cognitive

and information operations impact the spheres of societal influence. These will pertain to the spheres of societal influence and the use of offensive and defensive countermeasures and policies, which enables a more targeted and limited research and analytical process as well as areas of focus. In addition, the use of grounded theory as an analytical tool in this qualitative analysis is both helpful and necessary when creating cutoff points while ensuring both quality and depth in information while preventing bias within this paper.

Main Research Question:

- How are societal spheres of influence impacted by cognitive and information operations by hostile foreign malign adversaries and what can be done to improve U.S. offensive and defensive capabilities in a more volatile international system?

Additional Research Question #1:

- What are the societal spheres of influence and how can they be manipulated and influenced in the non-kinetic battlefield?

Additional Research Question #2:

- What are cognitive and information operations and how are they used for influencing and manipulating at the kinetic, non-kinetic, and multi-domain level?

Additional Research Question #3:

- What recent and previous approaches have been applied by the U.S. that focused on strengthening and adapting its offensive and defensive capabilities that pertain to countering cognitive and information operations by its foreign malign adversaries?

Additional Research Question #4:

- How should the U.S. improve and adapt its offensive and defensive capabilities in its cognitive and information operations in an international system where there is greater volatility than previously?

Hypothesis

- Increased volatility by hostile foreign malign adversaries in the international system requires the U.S. to strengthen and adapt its offensive and defensive capabilities to combat the threat.

Independent and Dependent Variables

- **Independent Variables:** Spheres of influence impacted by cognitive influence and information operations by foreign malign adversaries.
- **Dependent Variables:** Offensive and defensive capabilities currently being used and considered for countering adversarial malign cognitive influence and information operations.

Research Design

Purpose and Importance:

The purpose and importance of this qualitative research and analysis paper is intended to examine and ascertain the various threats and risks to U.S. national security regarding spheres of influence. In addition, it will pertain to the impact on the implementation of malign influence and information operations by adversarial and hostile foreign actors. This has continued to have both an impact and impairment on both the American societal spheres of influence, as well as its national security operational ability to deal with the ongoing threat landscape. In addition, this will also illustrate why it will be essential to examine policies and countermeasures currently

being utilized and potentially considered for application by practitioners and policymakers.

Lastly, the findings and analysis derived from this qualitative research paper will also address the need for an improved understanding and seriousness of this topic. After all, this paper seeks to address ongoing issues and concerns that have continued playing a significant role in impacting risk and threat management within a changing geopolitical and operational environment in real-time.

Theories:

Grounded Theory

Grounded theory is used for maintaining a targeted and limited focus in this qualitative analysis. This theory approach is considered a qualitative research methodology for analysis. In addition, it is inductive and formulated for examining a specific process or phenomenon, and the development of new theories based on the collection of real-world data and analysis (Lumivero 2023). Grounded theory enables a person to repeatedly connect and analyze data until theoretical saturation of themes, answered questions, and insights have been achieved. Common characteristics include simultaneous collection and analysis, grouping data into concepts, categories, and themes, and simultaneous development of those concepts, categories, and themes, which make the data collection process more cyclical and reflective (Deakin LibGuides 2023). Once this is achieved, the project will no longer require further data exploration and analysis. This is why grounded theory will enable a cutoff point for this qualitative research study, as it is also supported by an emphasis on the main and additional research questions that were identified in this paper. In addition, the cutoff points will help prevent the issue of bias from taking root in this paper with grounded theory via the maintenance of the targeted and focused nature of this qualitative analysis.

Realist Theory

The nature of this qualitative research analysis will be viewed with a realist lens, which is why the realist theory in international relations will be applied in this paper. After all, the themes of a volatile international system, malign influence, cognitive operations, information operations, societal spheres of influence, as well as offensive and defensive countermeasures and policies aimed at combatting and reversing them, are all based on real-world thinking and mindsets. The realist theory focuses on power being the predominant element in statecraft that produces the element of state survival (Cruz, Brabazon, Halfhill, and Ritzel 2020). The logic in this thinking is that realism has impacted the decisions of adversarial and hostile foreign actors to conduct cognitive and information operations on American societal spheres of influence, in addition to practitioners and policymakers being required to combat and counter them effectively.

Rational Choice Theory

Rational choice theory is another form of realism in international relations theory. However, it emphasizes that actors are both rational and serving their self-interests in international relations (Levin and Milgrom 2004). This means that the implementation of cognitive and information operations is being acted out on targeted rationality and self-interest in their agendas to impact societal spheres of influence. In addition, it not only relates to the realist theory but works collectively with it when paired with an analytical research topic that deals with both elements. Overall, this approach to combining rational choice and realist theories helps provide a lens that is clearer and more transparent for the reader when assessing the collected data and qualitative analysis. In addition, rationalism and realism can be utilized to help prevent bias taking root in this qualitative analysis that also incorporates grounded theory.

Research Methods

The incorporation of grounded theory in this qualitative analysis will enable it to assess relevant themes associated with this research project. This will require the creation of themes that are correlated with the research questions (main and additional questions) as well as the variables (independent and dependent variables). In addition, this research paper will examine the seven spheres of influence in society that are impacted by cognitive and information operations. It will explain examples of how they are impacted by adversaries to give the reader a coherent idea of the reality of the situation and the seriousness of the threats associated with them. There will also be a discussion on existing offensive and defensive capabilities used for countering cognitive and information operations as well as an exploration of ideas on adapting and improving them in an international system that is more volatile. Lastly, the research methods will utilize content analysis and case study assessments by utilizing this grounded theory approach to qualitative analysis that benefits examination purposes.

Data Collection Methods

Cognitive operations, information operations, and spheres of influence are not new topics and have been around for a long time throughout history. However, this qualitative study will collect data that spans several decades, periods, and eras. Data collection and assessments will start with the periods that signify the ending of World War II and the beginning of the Cold War era between the U.S. and the Soviet Union. In addition, data collection will begin in this period and continue to the current era in real-time. This means that data will be collected from the following eras: Cold War, Post-Cold War, Global War on Terror (GWOT), and Post Global War on Terror (Post GWOT).

It will be essential to collect and review data from these historical periods since there is a

story to tell in which the relationships illustrate a history of cause and effect that impacts future trends, catalysts, and events. This will be helpful to compare and contrast the differences between previous eras and the modern era, where high-tech innovations are more streamlined in cognitive and information warfare operations, such as artificial intelligence, deep fakes, generative art, social media, etc. This is why the data collection methods will review cycles and repetition of old versus new realities, situations, and scenarios. It will also collect data on the similarities and usages between the old and new methods in new and evolving scenarios, where it often raises questions regarding application versus misapplication. The examination of offensive and defensive cognitive and information operations capabilities by the U.S. national security and intelligence communities will also be required. In addition, it will look at the need to upgrade them to mitigate these threats in an international system that is more volatile with players like China and Russia who are prevalent in the non-kinetic area.

Data Sources:

This thesis will utilize open-source material from reputable sources such as RAND, War on the Rocks, Small Wars Journal, Long Wars Journal, Harvard University, American Military University, U.S. Department of Defense, Central Intelligence Agency, White House, Directorate of National Intelligence, Stratfor, Irregular Warfare Initiative, Modern War Institute, U.S. State Department, Center for Strategic and International Studies, National Defense University, Defense One, CI Centre, and MORS to name a few.

Data Analysis Process – Qualitative Analysis

The nature of this research project is centered on being a qualitative analytical product which is why grounded theory was applied. Qualitative research assumes that “individuals construct social reality in the form of meanings and interpretations, and that these constructions

tend to be transitory and situational” (Insites 2007). In addition, it is used to capture what is said about meanings and interpretations with data collected in narrative rather than numerical form like quantitative methods (Insites 2007). In fact, quantitative methods tend to be more limited in the ability to generate analysis of this type (Trochim 2024). This is where qualitative methods and analysis illustrate how data is analyzed emphasizing themes and patterns. In addition, it is also where grounded theory enables a simultaneous and repetitious relationship between the collection and analysis processes as well.

Overall, qualitative analysis incorporating grounded theory, realist theory, and rational choice theory is appropriate for this research project since the topic is ongoing, open-ended, and evolves in real-time. The impact of cognitive influence and information operations relating to the societal spheres of influence are regularly tracked and assessed by practitioners and policymakers. These are typically people who focus on the impact, how they are impacted, and the specific targeted purposes. Lastly, the development of defensive and offensive capabilities is also constantly assessed when dealing with countering cognitive influence and information operations by adversaries.

Analyzing the Data with Qualitative Analysis:

This qualitative study required the author to review data from different time periods. The ability to assess the data enabled the author to view it as both current and historical research to gain a full understanding of changing and evolving threats impacting U.S. national security that pertain to cognitive and information operations. This also required the author to review data about current and previous offensive and defensive capabilities to gain insight into what may be needed going forward in an international system that is more volatile. Since these themes and patterns have a history and are constantly evolving, it will require the author to discuss in greater

detail the following themes in the context of cognitive and information operations: societal spheres of influence, new international system or strategic reality, and offensive and defensive cognitive and information operations. These were discussed within the literature review and will be discussed in the facts and findings chapters of this paper.

Content analysis and case study formats will be utilized in these related sections to illustrate an understanding of themes such as: how spheres of influence are impacted by adversarial cognitive and information operations, offensive and defensive capabilities for cognitive and information operations, and evolving U.S. strategic reality in relation to current and emerging threats in a more volatile international system. In addition, the facts and findings chapter will also include a section discussing ways to mitigate rising threats in the cognitive and information operational arena that pertain to offensive and defensive capabilities. Since these illustrate ongoing issues and threats, this qualitative analysis will benefit from utilizing grounded theory, in addition to utilizing the realist and rational choice theories. The result will ideally enable the author to limit areas of focus in the addressed themes while utilizing realism to counter potential bias in the paper.

Lastly, the structure of the analysis will begin with the first section exploring how societal spheres of influence are impacted by malign adversaries' cognitive and information operations. This section assesses the relationship between various forms of non-kinetic warfare and their uses in the cognitive and human domains while putting them into context. In addition, the forms of non-kinetic warfare that will be discussed are the following: disinformation, political warfare, active measures, hybrid warfare, non-linear warfare, irregular warfare, unrestricted warfare doctrine, and three warfares strategy. There will be examples provided in these descriptions to help provide the reader with an understanding of how they are applied in

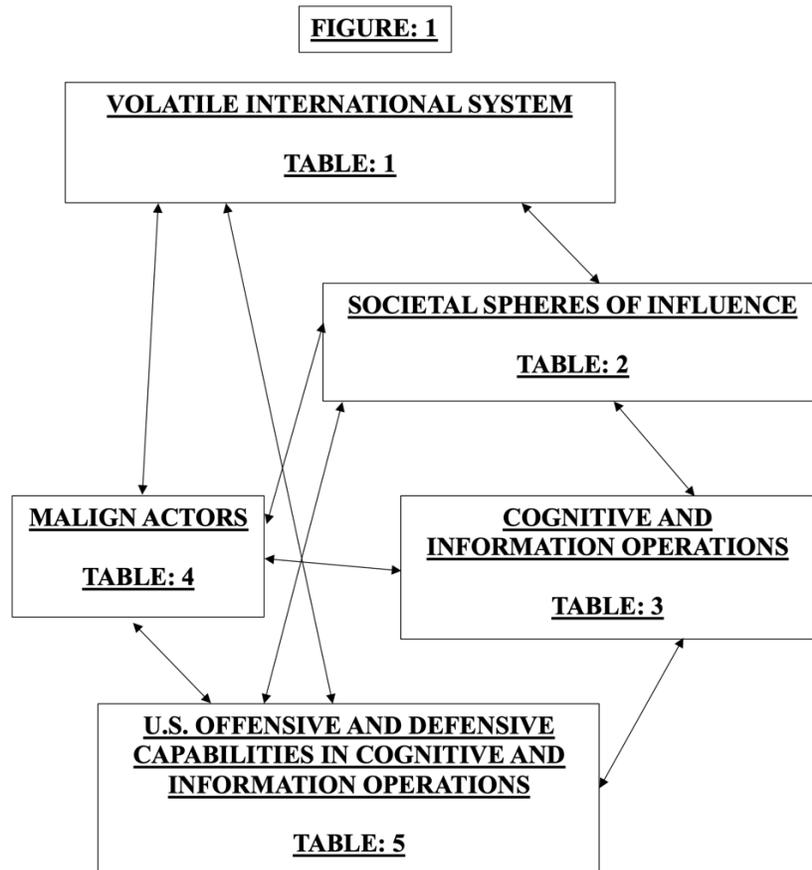
both foreign and domestic battlefields. Two case studies will follow this section that discuss how China incorporates its three warfares strategy in the South China Sea and how Russia executed hybrid and non-linear warfare in the 2014 annexation of Crimea, Ukraine. The last section will utilize this information and assess it while examining current weaknesses found in DoD's Military Information Support Operations (MISO) and areas for improving U.S. offensive and defensive capabilities that pertain to cognitive and information operations.

Coding Process:

Coding for grounded theory requires a cyclical data collection and analysis process. Since it is iterative, the research and analysis from the collected data will end when saturation has occurred. The codes used in this thesis are based on the research questions, aided in the focus on areas related to the themes and categories. Constant review and assessment were required to ensure data saturation was reached which resulted in identifying perspectives and key understandings of the issues, narratives, themes, and categories. For this coding process, a category was created by creating codes that served as themes and subcategories for codes. Since Grounded theory coding requires open coding, axial coding, and the eventual selective coding, this was helpful when undergoing the iterative process of collecting research, analyzing, and generating codes for further review and assessment (Delve and Limpaecher 2022). This was implemented at all levels, and the categories were given primary, secondary, and tertiary codes to represent the processes of open coding, axial coding, and selective coding applied throughout these processes.

Before the facts and findings process, it was imperative to ascertain a basis of understanding that would help answer the research questions. The tertiary coding process represents the beginning efforts, although not necessarily predominant from the start, since

grounded theory requires constant review and assessment at all levels of the research and analysis processes. However, once enough data was collected, the secondary codes were used as new coding categories that helped sharpen the image and focus on what would eventually become the primary code. The full assessment leading to the development of a new category is achieved once the primary code is codified via the secondary and tertiary coding processes. The categories created prior to the next stage of developing a grounded theory are the following: Volatile International System (Table: 1), Societal Spheres of Influence (Table: 2), Cognitive and Information Operations (Table: 3), Malign Actors (Table: 4), U.S. Offensive and Defensive Capabilities in Cognitive and Information Operations (Table: 5). While each of these categories are inter-related, it was assessed that some had a more direct correlation and linkages that can be shown below in Figure: 1.



These five categories underwent primary, secondary, and tertiary coding processes that underwent the open coding and axial coding processes. An equivalent to selective coding was used for compiling codes into becoming the primary code that would ultimately lead to the creation of a category. The coding for each of these five categories can be found below in Tables: 1 to 5. Afterward, it will be discussed how these categories evolved into the new codes and categories that make up the facts and findings portion.

TABLE: 1

VOLATILE INTERNATIONAL SYSTEM (Category) TABLE: 1						
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Tertiary Code</u>
Recent Periods	<i>Cold War Bipolar System</i>	<i>Post-Cold War Unipolar System</i>	<i>Post Global War on Terror (Post GWOT) (Current)</i>			
	(U.S. and Soviet Union) Dominated	(U.S.) Dominated	Increasing Multipolarity			<u>Tertiary Code</u>
	Block System	Globalization Interconnection/Multilateral	Increased Uncertainty			<u>Tertiary Code</u>
Increased Volatility	<i>Greater Competition</i>	<i>More State and Non-state Actors with strength, capabilities, and power projection</i>	<i>Increase in Global Proxy Conflicts</i>	<i>Increased Threat of Global and Regional Wars</i>	<i>Increase in Geopolitical Rivalries</i>	
	DIME (Diplomacy, Intelligence, Military, and Economic)	Non-kinetic and kinetic	Small Wars	Potential and Existing Conflicts	Old and New Rivalries Worldwide	<u>Tertiary Code</u>
Evolving U.S. Strategic Reality	<i>Power Projection</i>	<i>Dealing With More Players</i>	<i>U.S. Still Operating Under Unipolar Conditions</i>			
	More Difficult Than Previous Eras	Great Experience and Capabilities Than Previous Eras	Not upgraded to dealing with more actors with greater capacity, capabilities, and sophistication			<u>Tertiary Code</u>
	Greater Competition in DIME					<u>Tertiary Code</u>

TABLE: 2.1 and 2.2 (same category but split up in half)

SOCIETAL SPHERES OF INFLUENCE (Category) TABLE: 2.1			
Primary Code	<i>Secondary Code</i>	<i>Secondary Code</i>	<u>Tertiary Code</u>
Social, Family, and Friends	<i>Source for Unity and Belonging</i>	<i>Malign Influence Impact</i>	
	Community Stability	Cognitive and Information Operations	<u>Tertiary Code</u>
	Social Stability	Disrupting Social Fabric, Relationships, and Environments	<u>Tertiary Code</u>
	Family Stability	Creating Division and Confusion	<u>Tertiary Code</u>
Education and Training	<i>Source for Professional Growth, Development, Empowerment, and Direction</i>	<i>Malign Influence Impact</i>	
	Future	Cognitive and Information Operations	<u>Tertiary Code</u>
	Affects Attitude and Outlook	Disruption of Education and Training	<u>Tertiary Code</u>
	Replacement and Replenishment	Sabotage Workforce Replacement/Replenishment	<u>Tertiary Code</u>
Economic, Financial, and Workforce	<i>Source for Economy, Growth, and Development</i>	<i>Malign Influence Impact</i>	
	Prosperity	Cognitive and Information Operations	<u>Tertiary Code</u>
	Engine for Growth	Disruption of Economy	<u>Tertiary Code</u>
	Workforce Retention/Replenishment	Sabotage and Espionage	<u>Tertiary Code</u>
		Compromised Workforce and Economic System	<u>Tertiary Code</u>
Technology and Research and Development (R&D)	<i>Source for Economy, Growth, and Development</i>	<i>Malign Influence Impact</i>	
	Engine for Growth	Cognitive and Information Operations	<u>Tertiary Code</u>
	Engine for Prosperity and Jobs	Sabotage and Espionage	<u>Tertiary Code</u>
	New Innovations	Disruption in Systems	<u>Tertiary Code</u>
		Targeted Vulnerabilities	<u>Tertiary Code</u>
		Societal Over-reliance	<u>Tertiary Code</u>

SOCIETAL SPHERES OF INFLUENCE (Category) TABLE: 2.2

Primary Code	Secondary Code	Secondary Code	Tertiary Code
Information and Media	<i>Source for Being Informed, Knowledge, Communication, and Entertainment</i>	<i>Malign Influence Impact</i>	
	Online and Offline	Cognitive and Information Operations	<u>Tertiary Code</u>
	Awareness of the World and Surroundings	Societal Disruption	<u>Tertiary Code</u>
	Applies to Everything	Disinformation	<u>Tertiary Code</u>
		Misinformation	<u>Tertiary Code</u>
		Deepfakes	<u>Tertiary Code</u>
		False Positives	<u>Tertiary Code</u>
All Levels of Government	<i>Government Functions, Operations, and Programs</i>	<i>Malign Influence Impact</i>	
	Bureacracy	Cognitive and Information Operations	<u>Tertiary Code</u>
	Politics	Subversive Activity	<u>Tertiary Code</u>
	Branches of Government	Compromised Workforce	<u>Tertiary Code</u>
	Issues	Compromised Politicians	<u>Tertiary Code</u>
	Regulation	Compromised Systems	<u>Tertiary Code</u>
	Checks and Balances System	Disrupting Smoothness	<u>Tertiary Code</u>
	Security and Defense	Disrupting Progress in Initiatives	<u>Tertiary Code</u>
	National Pride and Influence	Causing Confusion	<u>Tertiary Code</u>
Warfare and Power Projection Capabilities	<i>Military, Intelligence, National Security, and Diplomacy</i>	<i>Malign Influence Impact</i>	
	Security and Defense	Cognitive and Information Operations	<u>Tertiary Code</u>
	Hard Power	Subversive Activity	<u>Tertiary Code</u>
	Soft Power	Sabotage and Espionage	<u>Tertiary Code</u>
	Training and Preparedness	Compromised Workforce	<u>Tertiary Code</u>
	Multi-domain	Compromised Systems	<u>Tertiary Code</u>
	Partners and Allies	Disrupting Smoothness	<u>Tertiary Code</u>
		Disrupting Progress in Initiatives	<u>Tertiary Code</u>
		Causing Confusion	<u>Tertiary Code</u>
		Causing Questioning of Loyalty and Effectiveness	<u>Tertiary Code</u>
		Unpreparedness of Surprise Scenarios	<u>Tertiary Code</u>
		Unreadiness for Scenarios	<u>Tertiary Code</u>

TABLE: 3

COGNITIVE AND INFORMATION OPERATIONS (Category) TABLE: 3				
Primary Code	<i>Secondary Code</i>	<i>Secondary Code</i>	<i>Secondary Code</i>	Tertiary Code
Doctrine	<i>Cognitive Warfare</i>	<i>Information Warfare</i>		
	Altering Target Populations Actions and Perceptions	Control of Flow and Access to Information		<u>Tertiary Code</u>
	Weaponization of Influence to Create Destabilization	Non-Kinetic		<u>Tertiary Code</u>
	Non-Kinetic	Subversive		<u>Tertiary Code</u>
	Cognitive Operations Implementation	Information Operations Implementation		<u>Tertiary Code</u>
Increase in Usage	<i>More Actors Implementing It</i>	<i>Benefits from Globalization</i>	<i>Evolving Multi-Polar System</i>	
	More Sophisticated Capabilities and Capacities	Stronger Economies	Increased Geopolitical Competition	<u>Tertiary Code</u>
	Plausible Deniability	More Muscles	Evolving Perceptions of Strengths and Weaknesses of Geopolitical Actors and Non-State Actors	<u>Tertiary Code</u>
	More Tempting to Use Than Conventional Means	Increased Power Projection		<u>Tertiary Code</u>
	Considered an Essential Tactic in Arsenals	Increased perception of Opportunities		<u>Tertiary Code</u>
	State Survival Purposes			<u>Tertiary Code</u>
Domestic Battlefield	<i>Public and Private Sectors Targeted</i>	<i>Weak and Strong Points</i>	<i>More Soft Targets</i>	
	Infrastructure	High Value Targets	Societal Spheres of Influence	<u>Tertiary Code</u>
	Key Individuals	Low Value Targets	Unprepared Sectors, Industries, and Leaders	<u>Tertiary Code</u>
	Systems	Unknowing population	Unknowing population	<u>Tertiary Code</u>
	Regular civilians	Less Prepared or Defendable	Less Prepared or Defendable	<u>Tertiary Code</u>
Foreign Battlefield	<i>Public and Private Sectors Targeted</i>	<i>Weak and Strong Points</i>	<i>More Variables Involved</i>	
	Infrastructure	Priority Targets	Less Controlled	<u>Tertiary Code</u>
	Key Individuals	High Value Targets	Increased Unkown Elements	<u>Tertiary Code</u>
	Systems	Low Value Targets	Greater Opposition	<u>Tertiary Code</u>

TABLE: 4

Malign Actors (Category) TABLE: 4				
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Tertiary Code</u>
Enemy	<i>State Actors</i>	<i>Non-state Actors</i>	<i>Unkown Adversary</i>	
	Non-Kinetic	Non-kinetic	Non-kinetic	<u>Tertiary Code</u>
	Kinetic	Kinetic	Kinetic	<u>Tertiary Code</u>
	Only Sovereign States	Wide Range of Potential Actors	Purpose and Malign Intention	<u>Tertiary Code</u>
	Purpose and Malign Intention	Purpose and Malign Intention	Plausible Deniability	<u>Tertiary Code</u>
	Plausible Deniability	Surprise/Unsuspected Action	Surprise/Unsuspected Action	<u>Tertiary Code</u>
	Vast resources and Capabilities	Limited Resources and Capabilities	Difficult to Notice or Track Immediately	<u>Tertiary Code</u>
Competitor	<i>Opportunistic</i>	<i>Gain an Edge</i>	<i>Cripple Competition</i>	
	Looking for Vulnerabilities	Operational Purposes	Tactical and Strategic	<u>Tertiary Code</u>
	Testing for Weaknesses	Strategic Focus	Systems (Online or Offline)	<u>Tertiary Code</u>
	Kinetic	Kinetic	Operational	<u>Tertiary Code</u>
	Non-Kinetic	Non-Kinetic	Kinetic	<u>Tertiary Code</u>
			Non-kinetic	<u>Tertiary Code</u>
Disruptor/Rogue Elements	<i>Outside the Box</i>	<i>Non-linear</i>	<i>Change Agent</i>	
	Patterns and Non-Patterns	Non-standeard Playbook	Ability to Alter Situations and Scenarios with Unique Approaches	<u>Tertiary Code</u>
	Unpredictable and Unorthodox Approaches	Re-define Rulebook	Doing the Opposite of Expected or Very Different	<u>Tertiary Code</u>
	New Perspectives	Multi-Disciplinary		<u>Tertiary Code</u>
	Unnoticed/Beyond Trained Eyes			<u>Tertiary Code</u>
Online	<i>Digital/Internet</i>	<i>Online Systems</i>	<i>Cyber</i>	
	Software Systems	Websites	Hacking	<u>Tertiary Code</u>
	Networks	Databases	Online Infrastructures and Components	<u>Tertiary Code</u>
	Online Media	Online Infrastructures and Components	Non-kinetic	<u>Tertiary Code</u>
	Social Media	Non-kinetic	Kinetic	<u>Tertiary Code</u>
	Kinetic			<u>Tertiary Code</u>
	Non-Kinetic	Kinetic		<u>Tertiary Code</u>
Offline	<i>Physical Infrastructure</i>	<i>Physical Systems</i>	<i>Non-cyber/Non-Digital</i>	
	Critical National Security Hard Assets	Machine Based	Analog System/Asset	<u>Tertiary Code</u>
	High Value Targets	Human Centered	Human Centered	<u>Tertiary Code</u>
	Mission Critical Assets	Tactical and/or Strategic Targets	Subversion	<u>Tertiary Code</u>
	Kinetic	Kinetic	Kinetic	<u>Tertiary Code</u>
	Non-Kinetic	Non-kinetic	Non-kinetic	<u>Tertiary Code</u>

TABLE: 5

U.S. OFFENSIVE AND DEFENSIVE CAPABILITIES (Category)				
IN COGNITIVE AND INFORMATION OPERATIONS TABLE: 5				
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Tertiary Code</u>
Cognitive Operations	<i>Psychology/Influence</i>	<i>Perception Management</i>	<i>Non-kinetic</i>	
	Targeted Group/Population	Communications Strategy	Digital and Analog	<u>Tertiary Code</u>
	Hearts and Minds	Cognitive Thinking	Multi-domain	<u>Tertiary Code</u>
Information Operations	<i>Information Management</i>	<i>Guide/Misguide</i>	<i>Inform/Disinform</i>	
	Controlling Information Flow	Tactical and/or Strategic Targets	Tactical and Strategic	<u>Tertiary Code</u>
	Narrative Warfare	Strategic Focus	Systems (Online or Offline)	<u>Tertiary Code</u>
	Kinetic	Kinetic	Operational	<u>Tertiary Code</u>
	Non-Kinetic	Non-Kinetic	Kinetic	<u>Tertiary Code</u>
			Non-kinetic	<u>Tertiary Code</u>
Defend and Counter Malign Threats	<i>Domestic</i>	<i>Foreign</i>	<i>U.S. Government</i>	
	National Security Interests	Overseas Interests and Assets	Department of Defense	<u>Tertiary Code</u>
	Critical National Security Infrastructures	Foreign Battlefield Scenarios	Intelligence Community	<u>Tertiary Code</u>
	Subversive and Black Swan Events	Online and Offline	National Security Enterprise	<u>Tertiary Code</u>
	Online and Offline		Online and Offline	<u>Tertiary Code</u>
More Competitive Environment than in Previous Periods	<i>More State and Non-state Actors Challenging U.S</i>	<i>Actors Have More Sophisticated Capabilities than in Previous Periods</i>	<i>Substituting Kinetic with Non-kinetic Currently</i>	
	Challenging U.S. Capacity and Capability	Globalization Improving Wealth and Investments in Capabilities	Kinetic War Prevention	<u>Tertiary Code</u>
	China and Russia are Predominant Players	Multi-domain Capabilities	Preparing for Potential Kinetic War But Not Ready for It	<u>Tertiary Code</u>
	Perceptions of Volatility Creating Weaknesses, Vulnerabilities, and Opportunities	Online and Offline	May Be Aligned with Partners and Utilizing it for Intelligence Purposes	<u>Tertiary Code</u>

New categories were developed after research and analysis occurred in Tables 1-5. The research in this stage illustrated similarities and interconnection linkages between the topics, themes, literature, information, and narratives about them. New research and analysis were cyclically conducted once these relationships were examined and identified. In grounded theory fashion, these processes went through iterative methods when developing primary, secondary, and tertiary codes that helped build up the level of research and understanding when saturation resulted in the development of new categories. The iterative coding process dealt with open coding, axial coding, and selective coding resulting in new categories and that contributed to developing the core category that created the basis for this thesis's hypothesis (Delve and Limpaecher 2022). Tables 1-5 resulted in the generation of three new categories, which are the following: Societal Spheres of Influence Impacted by Malign Adversaries (Table: 6), Application by Malign Actors: Methods of Disruption (Table 7), and Assessing MISO's Problems and Looking for Areas of Improvement (Table: 8).

The research and analysis conducted in Tables 6-8 were built on the previous work done in Tables 1-5. Correlations were noticed in Tables 6-8, just as had been observed in Tables 1-5, which illustrated linkages in relationships between the categories, codes (primary, secondary, and tertiary), and focus of this thesis. In addition, Figure 2 illustrates this relationship between the categories in Tables 6-8 and their relationships, correlations, and linkages with Tables 1-5. Data saturation occurred after iterative research, analytical, and coding methods were applied in a cyclical process and refined. Figure 2 illustrates how Tables 6-8 and their relationships with Tables 1-5 inter-relate and result in forming the hypothesis: Increased volatility by hostile foreign malign adversaries in the international system requires the U.S. to strengthen and adapt its offensive and defensive capabilities to combat the threat. Figure 2 can be viewed below in the

next part of this section, and Tables 6-8 will follow it afterwards.

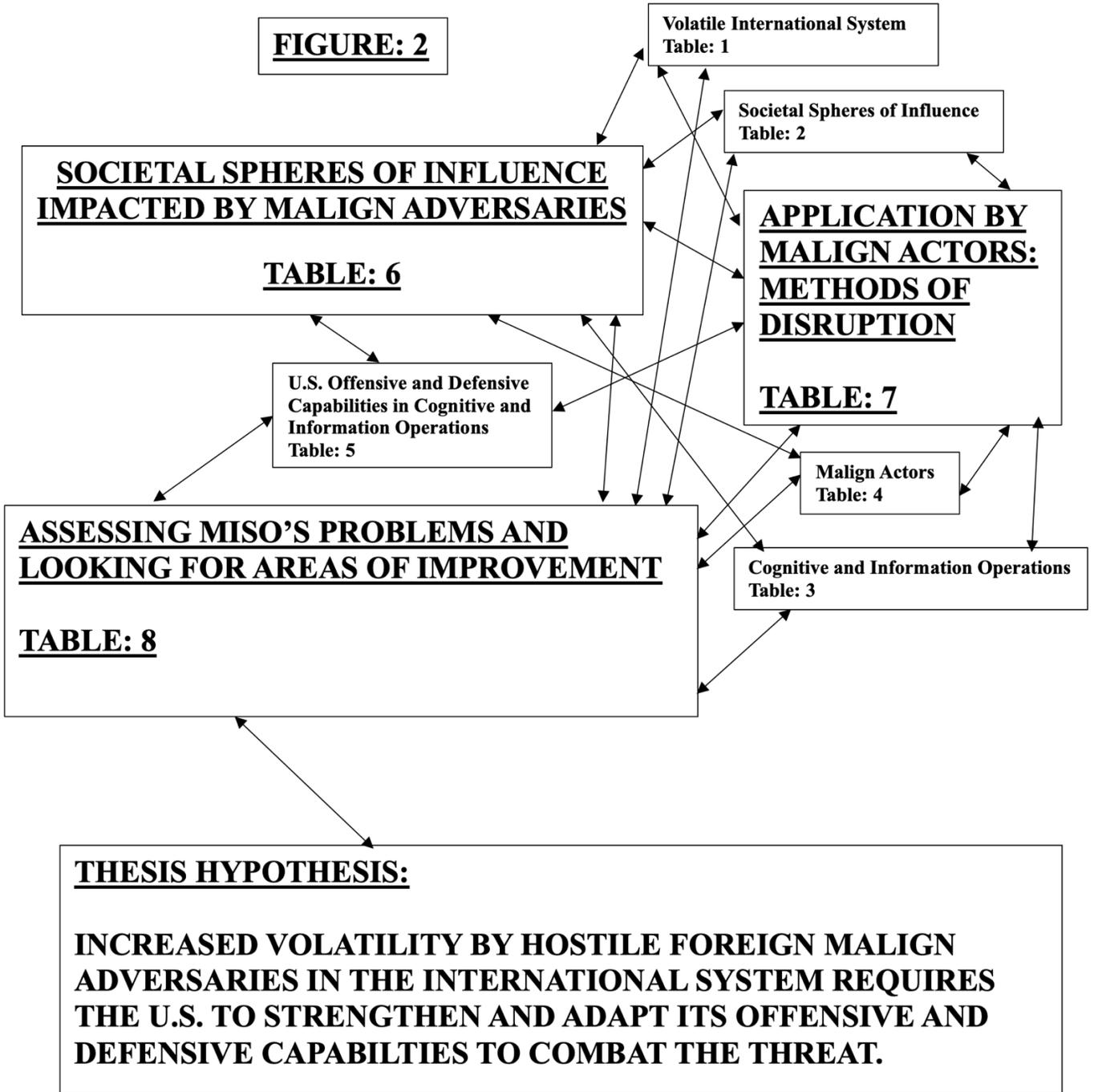


TABLE: 6

SOCIETAL SPHERES OF INFLUENCE (Category)					
IMPACTED BY MALIGN ADVERSARIES TABLE: 6					
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Tertiary Code</u>
Increasing Problems	<i>Growing Need to Understand the Problem</i>	<i>More Volatile International System</i>	<i>Strategic Reality</i>		
	Local, State, and National Levels	Growing Need to Upgrade Capabilities	Multi-polar		<u>Tertiary Code</u>
	Assess Known Vulnerabilities and Weaknesses	Increase in Capabilities	Increasing Threat of Major Conflicts in several hot zones		<u>Tertiary Code</u>
		Increase in Actors			<u>Tertiary Code</u>
Cognitive and Information Operations	<i>Cognitive and Human Domain of Warfare</i>	<i>Kinetic and Non-Kinetic</i>	<i>Online and Offline</i>		
	Multi-Domain	Foreign	Physical		<u>Tertiary Code</u>
	Mullti-disciplinary	Domestic	Non-physical		<u>Tertiary Code</u>
State or Non-state Actors	<i>Organization</i>	<i>Sovereign State</i>			
	Private Entity	China			<u>Tertiary Code</u>
	Business	Russia			<u>Tertiary Code</u>
	Political Group	Iran			<u>Tertiary Code</u>
	Terrorist Group	North Korea			<u>Tertiary Code</u>
	Partnerships and Alliances				<u>Tertiary Code</u>
	Criminal				<u>Tertiary Code</u>

TABLE: 7.1 and 7.2 (same category and primary code but split in half)

APPLICATION BY MALIGN ACTORS: (Category) TABLE: 7.1						
METHODS OF DISRUPTION						
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>		<u>Tertiary Code</u>
Methods of Disruption	<i>Disinformation</i>	<i>Political Warfare</i>	<i>Active measures</i>	<i>Hybrid Warfare</i>		
	U.S. China, Russia, Iran, etc.	U.S.	Soviet Union (Russia), U.S., and U.K.	Russia		<u>Tertiary Code</u>
	Professionalized and Whole-of-government Approach	Disinformation Operations Applying Whole-of-governement Approach	Disinformation Warfare Using Whole-of-government Approach and Permanent Wartime Mentality	Conventional, Irregular, Terrorist, and Criminal Measures		<u>Tertiary Code</u>
	Authoritarian vs. Liberal Democratic Systems Approaches	Generate Insurrections in Other Countries	Generate Insurrections in Other Countries	Mixture of Conventional and Unconventional		<u>Tertiary Code</u>
	Cognitive and Human Domain	Covert Political and Subversion Operations	Covert Political and Subversion Operations	Planned Accordingly Based on Battlefield Terrain Dynamics		<u>Tertiary Code</u>

TABLE: 7.2

APPLICATION BY MALIGN ACTORS: (Category) TABLE: 7.2						
METHODS OF DISRUPTION						
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Tertiary Code</u>
Methods of Disruption	<i>Non-Linear Warfare</i>	<i>Irregular Warfare</i>	<i>Unrestricted Warfare Doctrine</i>	<i>Three Warfares Strategy</i>		
	Russia	U.S., China, Russia, Iran, etc.	China	China		<u>Tertiary Code</u>
	Takes Hybrid Warfare and Adds Information, Cyber, Economic, Diplomatic, Political, and Social Measures	Unconventional Tactics and Strategy	More Emphasis on Unconventional over Conventional	Psychology, Media, Legal, and Public Opinion		<u>Tertiary Code</u>
	Disrupts Traditional Battlefield	Indirect and Asymmetrical	No barrier between soldier and citizen	Building Political and Geopolitical Power		<u>Tertiary Code</u>
	Non-military and Subversive Approach	Multi-domain Based	Digital and Physical Domain	Multi-domain Based		<u>Tertiary Code</u>

TABLE: 8

ASSESSING MISO'S PROBLEMS AND LOOKING (Category)					
FOR AREAS OF IMPROVEMENT			TABLE: 8		
<u>Primary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Secondary Code</u>	<u>Tertiary Code</u>
DOD Inspector General Report on Current State of MISO	<i>Declining Capabilities</i>	<i>Operational Decline Issues</i>			
	Cognitive and Information Operations	Training			<u>Tertiary Code</u>
	Information and Strategic Communications	Recruitment of Talent Decline			<u>Tertiary Code</u>
	Influence Operations	Overworked Staff			<u>Tertiary Code</u>
	Degrade Enemy Actions and Operations	Lack of Qualified Commanders			<u>Tertiary Code</u>
	Information Programs	Lack of Widescale MISO Status Assessment			<u>Tertiary Code</u>
	Lower Operational Success and Completion Levels	Workforce Retention Problem			<u>Tertiary Code</u>
	Utilizing Societal Spheres of Influence	Career Development Taking Too Long			<u>Tertiary Code</u>
		Creating Potential Human Capital Risk Threats			<u>Tertiary Code</u>
Recommendations for Improving MISO Offense and Defense Capabilities	<i>Do Updated Status Assessment</i>	<i>Recruit</i>	<i>Sharpen Skillsets</i>	<i>Adopt Wartime Mentality</i>	
	Morale	Within DOD	Additional Training	<i>Adversaries do the Same</i>	<u>Tertiary Code</u>
	Training and Retention	Private Sector	Continued Development	<i>Streamline Change</i>	<u>Tertiary Code</u>
	Capabilities and Capacity	University			<u>Tertiary Code</u>
	Staff Issues				<u>Tertiary Code</u>

Research Limitations

This is an endless and constantly evolving topic with a long history and narrative illustrating the changes that occur voluntarily, involuntarily, and out of necessity. The emerging nature of these issues and threats discussed will require the author to end the process of collecting and analyzing the data for this thesis. While the author attempted to limit the role of bias, it still is exhibited to some extent in this thesis. For example, the focus of this thesis will be U.S.-centric with the intention of helping shed light on these issues and concerns for the reader as well as practitioners and academics in the U.S. national security and intelligence communities. In addition, the data in this research will be solely based on information and insights found within the open-source realm. This means that this paper will utilize unclassified open-source material where limitations may occur unknowingly to this author.

Summary

The qualitative analytical method was appropriate for this research project rather than applying the quantitative numerical analytical method. It has more options and the ability to apply vast amounts of data as well as the ability to test and apply it thematically and categorically (Cleland 2017). In addition, the grounded theory is instrumental in ensuring there will be an endpoint in collecting and analyzing the data as well. Given the endless nature of this research topic, it was essential to apply the grounded theory to this qualitative analysis as well as not applying the mixed methods approach (qualitative and quantitative), which would have limited the data collection and analysis processes (Halcomb 2018). Lastly, the realist and rational choice theories were helpful to prevent bias that may result in the grounded theory method of analysis in this qualitative study.

However, there remain imperfections despite the qualitative analytical methods process

containing fewer limitations. The bias illustrated in this research study will be U.S.-centric, however, it will attempt to be as objective as possible. The emerging nature of the issues and threats that make up this topic deal with an evolving geopolitical threat landscape, which means there will be an eventual cutoff of data collection and analysis. Lastly, the research will be based on unclassified open-source material, which may have limitations, although a big picture lens will be useful in assessing the overall status of the prevailing issues, threats, and scenarios.

CHAPTER 4: FINDINGS & ANALYSIS

Overview

Understanding the state of U.S. offensive and defensive capabilities in cognitive and information operations requires the need to understand the various methods and strategies for conducting unconventional warfare. There will be a discussion on these methods and strategies used by adversaries of the United States, and they will be put into context in two case studies dealing with examples of non-kinetic warfare employed by China and Russia. Afterward, there will be a review of a recent Inspector General report of the U.S. Department of Defense (DoD) Military Information Support Operations (MISO) to find out why they are struggling and what recommendations can be made to improve their scenario outcome. Overall, there is concerning evidence that MISO is currently unable to perform its tasks at the level needed in an international system with more rivals that have sophisticated capabilities and have been investing in their cognitive and information operations.

Societal Spheres of Influence Impacted by Malign Adversaries

Both cognitive and information operations are utilized in non-kinetic and kinetic warfare. However, the cognitive domain can have elements of the human domain that can make it multi-domain related and multi-disciplinary in nature (Hofstetter and Jossen 2023). Societal spheres of influence can be found within it since elements of the human domain are part of this relationship. This means that societal spheres of influence are greatly impacted by the human domain that make up a wide range of areas in the humanities and social sciences throughout society (NATO Symposium 2021). Since the literature review showcased a wide range of areas that can make up societal spheres of influence, they will be categorized as the following: social, family, and friends; education and training; economic, financial, and workforce; technology and R&D;

information and media; arts and entertainment; all levels of government; warfare and power projection capabilities.

In addition, the current international system is showing signs of being more volatile, multi-polar, and consisting of greater adversarial threats than in previous periods. Mearsheimer reiterates this when he mentioned that hyper-globalization has reached a point that caused it to reverse the impacts going up, and that this period is witnessing a return to multiple rivalries that are both old and new (Mearsheimer 2019). Understanding the evolving nature of the changes in the systems as well as the strategic reality for the U.S. help shed light on understanding the type of methods, strategies, and doctrines that may be used against societies and their spheres of influence. This holds true if societal spheres of influence are targeted with the intention of causing disruption, panic, fear, and confusion via cognitive and information operations. As a result, this requires an examination of the elements that have been known for both their application and ability to impact and impair societies when malign actors utilize them for non-kinetic, kinetic, or multi-domain operations.

Disinformation, Political Warfare and Active Measures,

Modern-era disinformation operations evolved greatly during the inter-war years between the First and Second World Wars. The period from the 1920s to 1940s experienced major changes and enhancements in how disinformation operations both developed and distributed their content. In fact, they began to evolve into highly sophisticated operations that were conducted under a whole-of-government approach during conflicts and great power competition events (Rid 2020). Also, the inter-war years during this period went through major changes in journalism and overall communications with the popular use of radio in addition to print media. This period of disinformation warfare made the pace quicker and more cutthroat as well as being

more “innovative, conspiratorial, twisted, and nameless” until World War II and later decades made it professionalized with the increased relevance and streamlining by intelligence agencies and their strengthened bureaucratic structures (Rid 2020, 6-7).

During World War II and afterward, U.S. disinformation operations became known as “political warfare” and it eventually became identified as “active measures” by the former Soviet Union’s KGB in the 1950s during the Cold War (Rid 2020). Soviet-era active measures are described as disinformation campaigns that were designed to create and promote insurrections in other countries. It was considered a creation by the former Soviet Union’s KGB during the Cold War, but in practice it is much older. These operations were designed to be covert political operations with the permanent wartime mentality influencing this policy and practice. Galeotti mentioned that this practice was also utilized by the British and U.S. intelligence services during the Second World War and afterward. However, Galeotti also adds that active measures illustrated the Soviets’ ongoing wartime mentality as it described “a gamut of covert and deniable political influence and subversion operations, including (but not limited to) the establishment of front organizations, the backing of friendly political movements, the orchestration of domestic unrest and the spread of disinformation” (Galeotti 2019, 1).

In addition, Rid adds that all eras of disinformation possess the same goals, which were “to exacerbate existing tensions and contradictions within the adversary’s body politic, by leveraging facts, fakes, and ideally a disorienting mix of both” and that modern disinformation operations evolved into well-oiled, resourced, perfected, and managed processes by intelligence agencies (Rid 2020, 7). The more experienced agencies became, the more intense the competition evolved for all parties involved. Also, it impacted the rapidly growing need for agencies to adapt to changing trends, technologies, and internet culture, which Rid mentioned

had occurred after 2010 (Rid 2020). All state actors in the international system had to deal with these changes and U.S. adversaries realized the need to implement their disinformation operations at effective levels to be more competitive in the strategic realm of geopolitical influence.

China and Russia remain the two biggest adversaries that counter the U.S. with vast experiences in dealing with disinformation and malign influence campaigns (Kenney, Bergmann, and Lamond 2019). It is concerning since both states are regimes that exhibit authoritarian and nationalistic elements and find the liberal democratic system threatening to their governance, self-interests, and control of their societies. As a result, their operations tend to be geared toward attacking democracy and disrupting systems in the Western-led international order as well as casting doubt and faith in leadership (Robbins 2020). This is why they end up implementing disinformation operations against the U.S. public and private sectors as well as its leadership and citizens via these types of operations that pertain to the cognitive and human domains. These types of operations can greatly impact and impair societies if not countered effectively within an international system that is becoming more multi-polar and volatile.

Hybrid Warfare and Non-Linear Warfare

Hybrid warfare is considered a mixture of conventional and unconventional warfare methods that have evolved in the 21st century by modern-day Russia and China but were further developed by Russian General Valery Gerasimov. Ionita defines hybrid warfare to be the process of applying criminal, conventional, irregular, and terrorist measures to gain an advantage in a warzone against a conventional adversary (Ionita 2014). This form of warfare has been exhibited during the Russian incursions in Georgia as well as the ongoing Russo-Ukrainian war since 2014. However, it is also an approach that the People's Republic of China (PRC) has utilized in

its ongoing tensions with Taiwan in the South China Sea (Ball 2023). Smith mentions that hybrid warfare combines both conventional and unconventional methods that range from military operations, cyber warfare, disinformation campaigns, and economic pressure (Smith 2016). Whether it is a mixture of conventional or unconventional forces and strategic assets being applied, this form of warfare is a process that requires planning and understanding of the battle terrain while the target does not have to be only soldiers.

Non-linear warfare is a strategy aimed at disrupting the traditional battlefield making it more difficult to recognize the differences between combatants and civilians (Smith 2016). In addition, non-linear warfare also makes it more difficult to know the differences between war and peacetime through the implementation of cognitive and information operations. It is imperative to point out that non-linear warfare is often viewed as an extension of hybrid warfare since it has a broader geopolitical and strategic meaning that goes beyond it. In fact, the differences between hybrid warfare and non-linear warfare are that the former consists of only the following four methods, which are conventional, irregular, terrorist, and criminal, while the latter also adds the following four methods as part of the strategy: information, cyber, economic, diplomatic, political, and social (Schnauffer II 2017). The reason this evolved is because it became apparent that the Russians had outgrown the original definition of hybrid warfare during various engagements in multiple countries such as Ukraine, Syria, and throughout Europe (Schnauffer II 2017). Lastly, Morris paraphrases General Gerasimov when discussing this element of non-linear warfare when he said,

In short, ‘the very rules of war have been fundamentally changed’ and, according to General Gerasimov, non-military means have surpassed the power of force to achieve strategic and political goals. The current situation in Ukraine and, to some extent in neighboring former Soviet republics (primarily Baltic States), highlights the application of nonlinear war (Morris 2015, n.p.).

The overall impacts of hybrid and non-linear warfare can be dynamic due to the difficulty

of detecting and countering it in a timely manner to prevent it from disrupting the political, economic, and social fabric of societies (Kofman and Rojansky 2015). Whether it is the foreign or domestic battlefield, the spheres of influence in those areas will be greatly impacted and impaired since the goals utilize elements of cognitive and human domains to make the operation a strategic and tactical success. Also, since non-linear warfare strives to take a non-military and subversive approach to disrupting and weakening targets, it illustrates its roots in the policy of active measures despite not completely being the same. However, it illustrates a continued need for being able to respond and identify accordingly when having to deal with these methods, as well as knowing how to protect and counter them.

Irregular Warfare

Irregular warfare has been utilized by a wide range of countries, including China, Russia, Iran, and the United States, since conventional and nuclear war would be costly in terms of destruction and the number of lives that would ultimately be lost. However, countries that are applying irregular warfare are doing it to weaken systems and infrastructures which could make the wide-scale security environment more compromised and vulnerable to more threatening attacks (Jones 2021). The U.S. Irregular Warfare Technical Support Directorate defines irregular warfare as being the following:

Irregular Warfare is a struggle among state and non-state actors to influence populations and affect legitimacy. Irregular Warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will. It includes specific missions of unconventional warfare (UW), stabilization, foreign internal defense (FID), counterterrorism (CT), and counterinsurgency (COIN). Related activities such as military information support operations, cyberspace operations, countering threat networks, counter-threat finance, civil-military operations, and security cooperation also shape the information environment and other population-focused arenas of competition and conflict (IWTSD Website 2024, n.p.).

U.S. adversaries utilize irregular warfare since they may not be in the position of winning a conventional war. The other issue is that they may have studied U.S. doctrine regarding fighting irregular, conventional, or hybrid threats since they have over two decades of examining the data during the Global War on Terror (GWOT). As a result, U.S. adversaries have illustrated that they utilize the data they assess to “develop hybrid warfare styles to combat our distinct conventional military advantage” (Kirk 2023, 2). This illustrates the relationship that irregular warfare has with hybrid warfare and how it may be used for developing unconventional strategies in operations. Like hybrid and non-linear warfare, irregular warfare can be utilized for cognitive and information operations that can disrupt systems and societies.

Unrestricted Warfare Doctrine

Two Chinese colonels in the People’s Liberation Army (PLA) developed a war doctrine known as Unrestricted Warfare in 1999, which was a response to the way the U.S. successfully executed conventional warfare during the Persian Gulf War. Their argument was that “using armed forces to compel the enemy to submit to one’s will” no longer required conventional military methods and approaches (Barno and Bensahel 2016). In fact, the doctrine erased the barrier between soldiers and civilians, which essentially illustrates an endless potential for targets and battlefields that portray all areas of society and spheres of influence. Unrestricted Warfare also relates to all areas from the digital to physical domain making both the public and private sectors targets without realizing it until too late.

This is similar to the Russian doctrine pertaining to hybrid warfare, non-linear warfare, and active measures. However, it is different in the sense that it seeks to look at all options that are also considered unnatural and asymmetrical in use and adaptation that go beyond the realm

of conventional understanding (Gershaneck 2020). A successful attack incorporating this doctrine would not only be harmful but also greatly disruptive and very difficult for the military or civilian side to respond and counter within a timely manner. After all, it would likely take a decent amount of time to figure out what happened and act accordingly as well. In short, the many uses of unrestricted warfare can potentially be vast and range in all domains and spheres of influence within society due to the resourceful nature that this doctrine promotes (Gershaneck 2020).

Three Warfares Strategy

China's three warfares strategy is essentially their version of hybrid and non-linear warfare. However, Mattis mentions that their approach is different from the Russian version of hybrid warfare when observing their actions in the South China Sea as it is particularly geared toward building political power and influence in the region (Mattis 2018). Three warfares strategy deals with elements of psychology, media, legal, and public opinion which is a multi-dimensional approach to cognitive warfare without bringing in conventional or kinetic aspects (Takagi 2022). Stefan Halper specifically defines China's three warfares strategy as being the following:

1. ***Psychological Warfare:*** Seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations;
2. ***Media Warfare:*** Is aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests;
3. ***Legal Warfare:*** Uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be used to thwart an opponent's operational freedom and shape the operational space. It is also used to build international support and manage possible political repercussions of China's military (Halper 2013, 28).

Three warfares strategy is an influential disruptor as an element of Chinese soft power

projection throughout the international system. After all, these three concepts can be incorporated strategically and in sync with each other. Applying each of these strategies in a targeted and thoughtful manner can disrupt and cripple societies and systems as they also relate to the cognitive and human domain as well as cognitive and information operations. In addition, an example that Halper mentions about how China's three warfares can be used as an example is "If the U.S. objective [is] . . . to gain port access for the [U.S. Navy] in a particular country, for example, China would use the Three Warfares to adversely influence public opinion, to exert psychological pressure (i.e., threaten boycotts) and to mount legal challenges—all designed to render the environment inhospitable to U.S. objectives." (Halper 2023, 12). The example provided by Halper illustrated the level of complexity and the length the PRC would take to apply these types of cognitive and information operations to achieve a targeted outcome. In fact, it sheds light on how societal spheres of influence could not only be disrupted but also compromised if these styles of operations become unrecognized and lead to marginalization of the people and systems who may be impacted.

Operations Leading to Societal Disruption, Volatility, and Failure:

Case Study: China and Russia

The previous section illustrated the various methods and doctrines that are well-known and utilized by U.S. adversaries like China and Russia since they are predominant in their execution of these forms of warfare. A malign influence strategy that is a result of implementing cognitive and information operations in a society can be very disruptive to the efforts undertaken by the U.S. national security and intelligence communities (Yadav, Riedl, Wanless, and Woolley 2023). After all, systems, policies, analysis, and operations are only as effective as the level of protection and lack of being compromised that can impact results and success (Chin, Schaeffer,

Parker, and Janke 2023). However, the continuing geopolitical trends in the new international system illustrate an environment that is becoming more multi-polar, highly competitive, and filled with state and non-state actors with muscle and power projection capabilities.

These actors and entities can be utilized collaboratively and strategically to counter and undermine both U.S. operations and power projection capabilities domestically and abroad (Austin III 2023). In addition, foreign malign influence is becoming more crucial as a research topic about safeguarding spheres of influence in American society. This also includes systems as well as hearts and minds of the American population and its allies. The recent ODNI declassification of the role foreign actors like China, Russia, Iran, and Cuba played in intensifying efforts to influence the 2022 U.S. elections is an indication of this as well (ODNI Press Release 2023). There will be two case studies offered in this section to illustrate these concerns and how China and Russia have utilized variations of the non-kinetic warfare methods. Each of these case studies will provide a perspective and understanding on how they achieved a strategic and tactical outcome that also utilized elements of cognitive and human domain operations.

China Case Study - South China Sea Dispute

Territorial disputes in the South China Sea (SCS) have intensified since 2013 when the Peoples Republic of China (PRC) began reclaiming territory that had once been controlled by their predecessor, The Republic of China (now modern-day Taiwan). Reclaiming territory in the South China Sea is considered a national interest for the PRC as it pertains to national security and increasing their territorial integrity and realm of influence (Livermore 2018). In addition, the territory they are seeking to reclaim is called the Nine Dash Line island chain which consists of a majority of the South China Sea. The PRC has been seeking to reclaim the area for several years

since its formation in 1949, however, it also deals with territories that are either counter-claimed by other neighboring nations (i.e. Philippines, Vietnam, India, Taiwan, Indonesia, Brunei, Malaysia, Japan) or already considered sovereign owned by them as well (Global Conflict Tracker 2024). Lastly, these claims are not just about territory as they also pertain to rights regarding fishing access, control of natural resources in the sea, and control of trade routes.

This is a big predicament and obstacle for the PRC as the South China Sea is also among the busiest shipping routes in the world, and disruption would have a great impact on the global economy in terms of supply, logistics, and On-Demand business model. The South China Sea hosts 80% of global trade being transported through this region and the PRC's economic security is reliant on its preservation and stability since over 60% of its trade goods travel through these waters as well (China Power 2021). Despite the 2016 ruling by the United Nations Convention of the Law of the Sea (UNCLOS) that was in favor of the Philippines' complaint, the PRC chose not to accept the court's decision. The court ruled that the PRC had violated the UN Convention on the Law of the Sea by not respecting the Philippines' historic rights and entitlements to the sovereign territory (Permanent Court of Arbitration 2016).

However, the PRC has ignored this ruling as they continued efforts to reclaim land by a series of methods impacting territorial integrity and makeup of the physical domain. For example, the PRC continued efforts to increase the size of islands and create new islands as well as constructing new ports, military installations, and airstrips in an area known as the Paracel and Spratly Islands (Global Conflict Tracker 2024). These have become predominantly military installations which also impact the U.S. realm of influence in the South China Sea since it is the primary military power securing the trade routes in this region as well as enforcing a freedom of navigation policy. In addition, the PRC has also been known to establish an air defense

identification zone (ADIZ) in the East China Sea in 2013, which elevated concerns of their control of airspace that didn't legally belong to them (Pilger 2016). Lastly, territorial claims with the Philippines are still a problem given the history and intimidation tactics the PRC have executed to show a sign of force and intimidation, as well as testing the health of the 70-year defense pact between Manila and Washington (Shelbourne and Lagrone 2024).

In conclusion, the PRC has been employing its three warfares strategy to obtain territory in the South China Sea as well as gain a stronger foothold to strengthen its ability to challenge the United States' naval control of this region without entering into a kinetic conflict. Legal warfare and media warfare were applied by working within the UN framework as a signatory and publicly accepting the loss of the court ruling. However, Beijing also follows its own laws and mandates in mainland China, which illustrated its interpretation to contest the U.S. policy pertaining to freedom of navigation in the region and reversing it in their favor. Countering Washington's presence in the region also exhibited psychological warfare since it was trying to disrupt and raise doubt about the existing security structure and arrangements of that region. In particular, the level of tensions raised is not only testing the Philippines but also U.S. legitimacy in the area as well.

Russia Case Study – 2014 Annexation of Crimea, Ukraine

The Russian annexation of Crimea in 2014 illustrated elements of both hybrid and non-linear warfare by their military. Since it was an invasion, they had to offer legal grounds for the aggressions and interventions to portray relevance and legitimacy on the world stage (Kasapoglu 2015). Prior to the annexation, the Russian government's tensions with the Ukrainian government had intensified over eastern Ukraine (Donbas) and southern Ukraine (Crimea), which were largely ethnic-Russian-populated regions (Kononczuk 2014). The forces that entered

Crimea were a few thousand well-equipped troops that had an extensive 15,000 soldier support group from the Russian Black Sea Fleet, and a few thousand rallying demonstrators who were organized by a Russian organization known as the Russian Front (Kononczuk 2014). This group declared secession and dismissed the pro-Kyiv leadership while another armed group of unknown people had taken control of government buildings and critical infrastructures. At first, this did not seem like a military operation, but in the end, it resembled one. The unknown armed men who captured the infrastructures were Russian forces and nicknamed “little green men” afterward due to the mysterious nature of their identities at the time (Matissek 21).

During the annexation of Crimea, the Russian government also orchestrated a pro-Russia information operation that centered around using social media to influence the masses via propaganda, fear, narratives, and disinformation. The operation cost the Russians \$19 million and funded 600 people to comment and write on all types of media sites via social media (Holloway 2017). This information operations by the Russians were meant to sway opinions in other parts of the world and to help convince them of their policy objectives with Ukraine at the time. Although, their role was also meant to help gain supporters from the pro-Russian population in Crimea by spreading fear and hate of the Ukrainian government and its people. In addition to this social cyberattack incorporating strategic narratives, there were also significant Denial of Service cyberattacks on Ukrainian government websites and media outlets (Holloway 2017). There was also jamming of naval communications and Internet Protocol-telephonic attacks on government phones. This created a blackout event in which the citizens living in Crimea could not figure out what had occurred in real-time.

The incorporation of cognitive and information operations during the annexation of Crimea was considered a success for the Russian military and was an eye opener for the U.S. and

its allies regarding Russia's approaches to hybrid and non-linear warfare. In this case, the Russians had redefined the battlefield to prevent extensive loss of life from this coup while maneuvering geopolitical risks simultaneously. However, the use of real soldiers and forces that seemed unconventional or equivalent to being "little green men" was very helpful in creating the element of surprise and confusion among the population and adversarial Ukrainian forces. Lastly, the information operations using both types of cyber during the Crimean Annexation had also proved to be impactful at being disruptive and causing confusion, chaos, and uncertainty to the extent that cognitive warfare kept the public from getting too involved.

U.S. Offense and Defense Capabilities in Cognitive and Information Operations:

Assessing MISO's Problems and Areas for Improvement

A March 25, 2024 evaluation by the U.S. Department of Defense (DoD) Inspector General published a report discussing the declining capabilities of its Military Information Support Operations (MISO). MISO is crucial for DoD since it pertains to executing cognitive and information operations for strategic and tactical purposes that counter efforts by malign actors and adversaries. DoD's Joint Publication 3-13.2 notes that Military Information Support Operations (MISO) utilize information and strategic communications for the purpose of influencing targeted groups by promoting themes to change their attitudes and behaviors. In addition, MISO also utilizes information and cognitive operations to degrade an enemy's combat strength, civilian interference reduction, collateral damage control, and increase population support for operational purposes (DoD Joint Publication 3-13.2). An operation using MISO can help a military commander utilize designed information programs that can be used for influencing political, military, economic, social, information, and infrastructure that is related to the operational environment (DoD Joint Publication 3-13.2). Lastly, the multi-domain nature of

MISO illustrates its potential in performing offensive and defensive operations to counter malign adversarial near-peer actors like China and Russia who operate their versions of non-kinetic warfare as well.

The societal spheres of influence are represented in the MISO function, and it is necessary for carrying out operations in the kinetic and non-kinetic battlefield since the targets could be individuals, groups, enemies, adversaries, friendly, and neutral. Furthermore, this is why having a strong cognitive domain is considered to be a valuable asset since it would be helpful to have greater maneuverability to deal with psychological strengths, patterns, behaviors, and motivations of an adversary or target population (McClenon 2023). These findings will be discussed in the next section as they illustrate the current state of MISO or at least what DoD is willing to publish at this juncture. However, the messaging indicates that there is a significant need for updating its role and capacity to meet the increasing adversarial non-kinetic threats occurring in an international system that is more multi-polar and volatile. Once these are addressed, there will be a section discussing recommendations for improving MISO, which will impact its offensive and defensive capabilities.

MISO: State of Operational Decline

The report by the DoD Inspector General indicated that there is a serious problem with the recruitment, training, and retention of military personnel needed to conduct MISO. In addition, it mentioned that not only was MISO lacking in their special operations workforce for performing the Psychological Operations (PSYOP) but also for non-special operations staff members (DoD Inspector General 2024, i). Army Reserves are being utilized to fill in the gap in manpower. However, the workforce remained low and only 25% of PSYOP groups were required to complete their missions (DoD Inspector General 2024, i). This is problematic as it

raises serious issues about the ability of MISO to fulfill its mission mandate and the ability to address staffing concerns.

Other concerning issues deal with an overworked workforce and staff either not possessing or taking too long to update their skillsets due to limitations in the Army officer career management policy. Limitations in this policy will not allow newly commissioned officers to serve in MISO's PSYOP branch, thus having fewer PSYOP-qualified commanders due to the number of years of training it would take once accepted (DoD Inspector General 2024, i). Lastly, MISO has not conducted the necessary assessments for determining current capabilities, force projection, readiness, and information needed for determining staff replenishment, growth, and sustainment of career employees (DoD Inspector General 2024, i). The dilemma this raises is not only the potential for burnout of specially trained soldiers but also a serious morale problem that illustrates a vulnerability in the DoD that U.S. adversaries can take advantage of. For example, it provides an opportunity for an adversary with sophisticated cognitive and information operations to penetrate and overrun any weaknesses in MISO operations due to a lack of manpower and properly trained staff. Another example could be the idea of taking advantage of staff that may have low morale, burnout, overworked, and disgruntled who could be used for potential espionage situations.

MISO: Recommendations for Improving Offense and Defense Capabilities

These are serious issues for MISO as they are currently understaffed while employees are not properly matched with the range of global competitors that have spent sizable resources in their budgets for conducting irregular and conventional warfare with their cognitive and information operations capabilities. In addition, not being prepared takes away the opportunity to find an adversary's vulnerability, which is easy to find in authoritarian political systems that

have poor human rights records with their population (Jones 2021). MISO needs to do a much-needed assessment of their current capabilities based on staff size, qualified talent, and the streamlined advanced entry of potential talent that wants to work for the organization but is unable due to current policy guidelines. This also signifies the need for MISO to adopt more of a wartime mentality to perform the necessary changes in a streamlined fashion while recruiting from the talent pool within DoD, the private sector, and at the university level. Cognitive and information operations deal with the human domain, which requires a need for professionals with multiple skillsets and are multidimensional as well. After all, irregular warfare requires this element for the offensive and defensive capabilities to be always sharpened.

CONCLUSION

The international system is now more volatile and requires the U.S. to update its capabilities and capacities in the cognitive and human domains. Cognitive and information operations were a key focus in this thesis, however, this is a topic that is vast and filled with additional areas of focus. However, this thesis sought to address the questions of whether the U.S. needed to improve its cognitive and information operations and how societal spheres of influence can be impacted by them via malign foreign adversaries. The research in this thesis not only proves that the hypothesis is correct but that the situation regarding U.S. readiness and capability to counter serious malign attacks in the cognitive and human domains will have limitations and require capacity upgrades. Although this is not a short-term fix, there remain various ways to improve the situation, capability, and capacity regarding the state of MISO.

In addition, this qualitative analysis assessed the current state of MISO in the context of the data that was reviewed in the findings as well as content in the literature review. The literature review assessed the arguments pertaining to the international system becoming more multi-polar and the reasons why that is the case. They range from globalization creating stronger actors, the long-term development of the China-Russia relationship, Russia's Primakov doctrine, and the concept of living in a Post-Global War on Terror era (Post GWOT). Other areas of the literature review delved into the debate regarding the cognitive versus human domain in multi-domain warfare as well as improving offensive and defensive capabilities in cognitive and information operations. Each of these was helpful in assisting the author in answering both the primary and additional questions and serving as a compass for areas of focus in the research process.

The use of grounded theory as well as the realist and rational choice theories were

helpful. As mentioned earlier, this qualitative analysis using grounded theory is ideal since a combination of each one enables a wide range of research areas that could be explored while creating the cutoff point. However, grounded theory still runs the risk of bias, and the author added the realist and rational choice theories in international relations. This enabled the author to manage and limit bias since this thesis has a U.S.-centric focus. However, the author found this approach useful as it assumes that the type of actors implementing non-kinetic operations that incorporate cognitive and information operations against the U.S. are rational, pragmatic, and doing it out of self-interest and survival.

Assessing these areas led to the buildup of the focus in the facts and findings chapter of this thesis. The manner it was done in this chapter was geared for building up to the last section dealing with DoD's Military Information Support Operation (MISO). It first addressed well-known strategies and doctrines by U.S. adversaries such as China and Russia (and the U.S.) and discussed in detail what they were and how they could be used to manipulate societal spheres of influence. The strategies and doctrines discussed were the following: disinformation, political warfare, active measures, hybrid warfare, non-linear warfare, irregular warfare, unrestricted warfare, and three warfares strategy. The discussion on each of these led to the two case studies that dealt with how China utilized its three warfares strategy in the South China Sea and how Russia implemented hybrid and non-linear warfare to annex Crimea, Ukraine in 2014. This was helpful to review and put into context to assess MISO and its current state.

The assessment of MISO is that it needs proactivity and streamlining in addressing the concerns the Inspector General's report had on the state of their workforce. At this current juncture, MISO is understaffed and overworked, and its protocols are preventing quicker access to new employees due to rules about entry for newly commissioned officers. This is particularly

problematic in the sense that developing highly skilled cognitive and information soldiers with PSYOP training takes years to develop in a period where time may not always be abundant. Non-kinetic wars have a habit of turning into kinetic wars and MISO is designed for both types. The organization needs to do major assessments on their current capacity as well as areas dealing with workforce training, retention, and morale. This is a critical issue as MISO is currently not finishing all its missions due to limited staff and qualified professionals to carry it out.

MISO needs to reach out and allow qualified candidates within DoD who are interested in this profession and begin developing them after the hiring rules have been updated. In addition, they should also recruit professionals and students who are in either the public sector or in universities. If they recruit university students, it will be helpful to ascertain the programs that could be considered desirable based on degree programs and accomplishments as well as traits and worldview. However, worldview will always need to be considered in all areas for consideration as the cognitive and human domain in the new international system requires critical thinkers who also have multidisciplinary and multidimensional mindsets. After all, it is an approach utilized by U.S. adversaries to undermine it via their execution of cognitive and information operations.

AREAS FOR FUTURE RESEARCH

1. Streamlining MISO workforce buildup and quicker access to training.
2. Recruitment increases and workforce retention program at MISO.
3. Assessing the current state and capacity of MISO and developing a plan for improving functioning rates over a period.
4. Working with inter-agency organizations to improve capacity for cognitive and information operations.
5. Developing simulations and tabletop exercises for training and career development regarding cognitive and human domain elements.
6. Mapping out known cases of adversary malign influence operations in multiple domains and sectors that incorporate multidisciplinary and multi-dimensional approaches.
7. Improving the resiliency of the societal spheres of influence that are vulnerable to becoming targets by adversarial malign actors.

LIST OF REFERENCES

- Allison, Graham. 2020. "The New Spheres of Influence: Sharing the Globe with Other Great Powers." *Www.hks.harvard.edu. Foreign Affairs*. March 1, 2020. https://www.hks.harvard.edu/sites/default/files/HKSEE/HKSEE%20PDFs/Allison_Spheres%20of%20Influence%2C%20Foreign%20Affairs%2C%20March-April%202020.pdf.
- Austin III, Lloyd J. 2023. "Strategy for Operations in the Information Environment." US DOD. July 2023. <https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF>.
- Backes, Oliver, and Andrew Swab. 2019. "Cognitive Warfare the Russian Threat to Election Integrity in the Baltic States." *Harvard Kennedy School Belfer Center*. Cambridge, Massachusetts: Harvard. <https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf>.
- Ball, Joshua. 2023. "The Changing Face of Conflict: What Is Hybrid Warfare?" *Global Security Review*. August 2023. <https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/>.
- Barno, David, and Nora Bensahel. 2016. "A New Generation of Unrestricted Warfare." *War on the Rocks*. April 19, 2016. <https://warontherocks.com/2016/04/a-new-generation-of-unrestricted-warfare/>.
- Bernal, Alonso, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla. 2020. "Cognitive Warfare: An Attack on Truth and Thought." *NATO Innovation Hub*. 2020. <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf>.
- Biden, Pres. Joe. 2021. "Remarks by President Biden on the End of the War in Afghanistan." *The White House*. August 31, 2021. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/>.
- Branch, Austin, Ed Cardon, Devin Ellis, and Adam Russell. 2021. "We Ignore the Human Domain at Our Own Peril." *Modern War Institute*. June 14, 2021. <https://mwi.westpoint.edu/we-ignore-the-human-domain-at-our-own-peril/>.
- Brose, Christian. 2020. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York: Hachette Books.
- Center for Preventive Action. 2024. "Territorial Disputes in the South China Sea." *Global Conflict Tracker*. Council on Foreign Relations. March 19, 2024. <https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea>.

- Claverie, B., B. Prebot, and F. Du Cluzel. 2021. "Cognitive Warfare: The Future of Cognitive Dominance." NATO. Science and Technology Organization. June 21, 2021. <https://hal.science/hal-03635898/document#:~:text=Chapter%20%20%E2%80%93%20COGNITIVE%20DOMAIN%3A%20A%20SIXTH%20DOMAIN%20OF%20OPERATIONS%3F&text=>.
- Cleland, Jennifer Anne. 2017. "The Qualitative Orientation in Medical Education Research." *Korean Journal of Medical Education* 29, no. 2 (May): 61–71. <https://doi.org/10.3946/kjme.2017.53>.
- Chin, Christopher H., Nicholas P. Schaeffer, Christopher J. Parker, and Joseph O. Janke. 2023. "When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force." National Defense University Press. NDU Press. May 4, 2023. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3379870/when-dragons-watch-bears-information-warfare-trends-and-implications-for-the-jo/>.
- China Power. 2025. "How Much Trade Transits the South China Sea?" ChinaPower Project. CSIS. January 25, 2025. <https://chinapower.csis.org/much-trade-transits-south-china-sea/>.
- Cohen, Ariel. 2001. "The Russia-China Friendship and Cooperation Treaty: A Strategic Shift in Eurasia?" The Heritage Foundation. July 18, 2001. <https://www.heritage.org/europe/report/the-russia-china-friendship-and-cooperation-treaty-strategic-shift-eurasia>.
- Cohen, Ariel . 1997. "The 'Primakov Doctrine': Russia's Zero Sum Game with the United States." The Heritage Foundation. December 15, 1997. <https://www.heritage.org/report/the-primakov-doctrine-russias-zero-sum-game-the-united-states>.
- Cruickshank, Ian, Kirk Windmueller, and Matt Benigni. 2023. "Reaching the Tipping Point: Lessons from Combining Kinetic and Information Operations." Irregular Warfare Initiative. July 19, 2023. <https://irregularwarfare.org/articles/reaching-the-tipping-point-lessons-from-combining-kinetic-and-information-operations/>.
- Cruz, Col. Miguel A. , Capt. John J. Brabazon, Col. DeDe S. Halfhill, and Col. Scott M. Ritzel. 2020. "Between Theory and Practice: The Utility of International Relations Theory to the Military Practitioner > Air University (AU) > Article Display." Air University. Wild Blue Yonder Online Journal. February 3, 2020. <https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2063140/between-theory-and-practice-the-utility-of-international-relations-theory-to-th/>.
- Delve, LaiYee Ho, and Alex Limpacher. 2022. "How to Do Open, Axial, and Selective Coding in Grounded Theory." Delve. February 8, 2022. <https://delvetool.com/blog/openaxialselective>.

- Dundon, Molly. 2021. "INFORMATION WARFARE in the HIGH-END FIGHT." *Naval Post Graduate School*. Monterey, California: Naval Post Graduate School.
<https://apps.dtic.mil/sti/trecms/pdf/AD1150927.pdf>.
- "Evaluation of the DoD Military Information Support Operations Workforce." 2024. *Defense.gov*. DoD. https://media.defense.gov/2024/Mar/27/2003421651/-1/-1/1/DODIG-2024-068_REDACTED_SECURED.PDF.
- "Factsheet: War on Terror." 2023. Bridge Initiative at Georgetown University. August 1, 2023.
<https://bridge.georgetown.edu/research/factsheet-war-on-terror/>.
- Fingar, C. Thomas. 2008. "2025 Global Trends Final Report." *Directorate of National Intelligence*. National Intelligence Council.
https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf.
- Gabuev, Alexander. 2023. "What's Really Going on between Russia and China." *Foreign Affairs*, April 12, 2023. <https://www.foreignaffairs.com/united-states/whats-really-going-between-russia-and-china>.
- Galeotti, Mark, "Active Measures: Russia's Covert Geopolitical Operations," *Marshall Center Security Insight*, no. 31, June 2019,
<https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0>.
- Gershaneck, Kerry. 2020. "To Win without Fighting." *Www.usmcu.edu*. Marine Corps University. June 17, 2020. <https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/To-Win-without-Fighting/>.
- Gregg, Heather S. 2016. "The Human Domain and Influence Operations in the 21st Century." *Special Operations Journal* 2, no. 2 (July): 92–105.
<https://doi.org/10.1080/23296151.2016.1239978>.
- Halcomb, Elizabeth J. 2018. "Mixed Methods Research: The Issues beyond Combining Methods." *Journal of Advanced Nursing* 75, no. 3 (December): 499–501.
<https://doi.org/10.1111/jan.13877>.
- Hall, Daniel. 2023. "America Must Engage in the Fight for Strategic Cognitive Terrain." *JFQ* First Quarter, no. JFQ 108: 75–86.
https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-108/jfq-108_75-86_Hall.pdf?ver=FLLYShQtZDArhRfRVKgdmw%3d%3d.
- Halper, Stefan. "CHINA: The Three Warfares." *Cryptome*. 2013. Accessed May 27, 2017. <https://cryptome.org/2014/06/prc-three-wars.pdf>.

- Hofstetter, LTC Patrick, and CAPT Flurin Jossen. 2023. "There Is No Need for a Cognitive Domain." TDHJ.org. The Defence Horizon Journal. November 2, 2023. <https://tdhj.org/blog/post/no-need-cognitive-domain/>.
- Holloway, Michael. 2017. "How Russia Weaponized Social Media in Crimea." The Strategy Bridge. May 10, 2017. <https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>.
- Howard, Michael, Peter Paret, and Carl Von Clausewitz. 1984. *Carl von Clausewitz on War*. Princeton, Nj: Princeton University Press; Revised ed. edition (June 1, 1989).
- "Joint Publication 3-13.2 Military Information Support Operations." 2014. DOD. DOD. November 2014. https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/Military_Information_Support_Operations.pdf.
- Ionita, Craisor-Constantin. 2014. "Is Hybrid Warfare Something New?" *Strategic Impact* 4, no. 53: 61–71. <https://www.proquest.com/docview/1692921983?sourcetype=Scholarly%20Journals>.
- Irwin, Douglas. 2022. "Globalization Enabled Nearly All Countries to Grow Richer in Recent Decades." Peterson Institute for International Economics. June 16, 2022. <https://www.piie.com/blogs/realtime-economic-issues-watch/globalization-enabled-nearly-all-countries-grow-richer-recent>.
- Jensen, Benjamin, and Divya Ramjee. 2023. "Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs." Www.csis.org. December 20, 2023. <https://www.csis.org/analysis/beyond-bullets-and-bombs-rising-tide-information-war-international-affairs>.
- Jones, Seth. 2021. "The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare." CSIS. February 4, 2021. <https://www.csis.org/analysis/future-competition-us-adversaries-and-growth-irregular-warfare>.
- Kasapoglu, Can. 2015. "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control Introduction: A Renewed Russian Military Thinking." *NATO Research Paper*. NATO. https://www.files.ethz.ch/isn/195099/rp_121.pdf.
- Kenney, Carolyn, Max Bergmann, and James Lamond. 2019. "Understanding and Combating Russian and Chinese Influence Operations." Center for American Progress. February 28, 2019. <https://www.americanprogress.org/article/understanding-combating-russian-chinese-influence-operations/>.

- Kessler, Sam. 2022. "The Multi-Polar Role of Russia's Primakov Doctrine and the Certainty of a Chinese-Russian Strategic Alliance - by Sam Kessler." Fulcrum Global. Society for Defense and Strategic Studies (SDSS) at AMU/APUS. December 14, 2022. <https://fulcrumglobal.us/the-multi-polar-role-of-russias-primakov-doctrine-and-the-certainty-of-a-chinese-russian-strategic-alliance/>.
- Kirk, Jacob A. 2023. "Irregular and Hybrid Warfare." NCO Journal. Army University Press. July 24, 2023. <https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2023/July/Irregular-and-Hybrid-Warfare/>.
- Kofman, M., & Rojansky, M. (2015). A Closer Look at Russia's "Hybrid War." Kennan Cable No. 7. Woodrow Wilson International Center for Scholars.
- Konończuk, Wojciech. 2014. "Russia's Real Aims in Crimea." Carnegie Endowment for International Peace. March 14, 2014. <https://carnegieendowment.org/2014/03/13/russia-s-real-aims-in-crimea-pub-54914>.
- Kuehl, Daniel T. 2002. "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age." *International Law Studies* 76, no. 1 (January): 23. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils>.
- Layne, Christopher. 1997. "From Preponderance to Offshore Balancing: America's Future Grand Strategy." *International Security* 22, no. 1 (July): 86–124. <https://doi.org/10.1162/isec.22.1.86>.
- Levin, Jonathan, and Milgrom, Paul. "Introduction to Choice Theory." Stanford University. September 2004. Accessed May 28, 2017. <http://web.stanford.edu/~jdlevin/Econ%20202/Choice%20Theory.pdf>.
- Livemore, Doug. 2018. "China's 'Three Warfares' in Theory and Practice in the South China Sea." Georgetown Security Studies Review. March 25, 2018. <https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/>.
- Lumivero. 2023. "An Overview of Grounded Theory Qualitative Research." Lumivero. December 1, 2023. <https://lumivero.com/resources/blog/an-overview-of-grounded-theory-qualitative-research/>.
- MacDonald, Maj. Andrew, and Maj. Ryan Ratcliffe. 2023. "Cognitive Warfare: Maneuvering in the Human Dimension." *Proceedings Online* 149/4, no. 1442 (April). <https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension>.

- Matissek, Jahara. 2021. "From Little Green Men to Little Blue Helmets: Imagining the Future of Russian Aggression—and What to Do about It." Modern War Institute. November 2, 2021. <https://mwi.westpoint.edu/from-little-green-men-to-little-blue-helmets-imagining-the-future-of-russian-aggression-and-what-to-do-about-it/>.
- Mattis, Peter. 2018. "China's 'Three Warfares' in Perspective." War on the Rocks. January 30, 2018. <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>.
- McClenon, Julia M. 2023. "We're WEIRD and Our Adversaries Know It: Psychological Biases Leave the United States Vulnerable to Cognitive Domain Operations." Irregular Warfare Initiative. June 7, 2023. <https://irregularwarfare.org/articles/were-weird-and-our-adversaries-know-it-psychological-biases-leave-the-united-states-vulnerable-to-cognitive-domain-operations/>.
- Mearsheimer, John J. 2019. "Bound to Fail: The Rise and Fall of the Liberal International Order." *International Security* 43, no. 4 (April): 7–50. https://doi.org/10.1162/isec_a_00342.
- Miller, Seumas. 2023. "Cognitive Warfare: An Ethical Analysis." *Ethics and Information Technology* 25, no. 3 (September). <https://doi.org/10.1007/s10676-023-09717-7>.
- Morris, Victor R. 2015. "Grading Gerasimov: Evaluating Russian Nonlinear War through Modern Chinese Doctrine ." Smallwarsjournal.com. Small Wars Journal. September 17, 2015. <https://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine>.
- Nettis, Kimber. 2020. "Multi-Domain Operations: Bridging the Gaps for Dominance." Www.airuniversity.af.edu. March 16, 2020. <https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2109784/multi-domain-operations-bridging-the-gaps-for-dominance/>.
- Nye, Joseph S. 2013. "What China and Russia Don't Get about Soft Power." Foreign Policy. Foreign Policy. April 29, 2013. <https://foreignpolicy.com/2013/04/29/what-china-and-russia-dont-get-about-soft-power/>.
- "ODNI Releases Intelligence Community Assessment of Foreign Threats to the 2022 U.S. Elections." December 18, 2023. www.dni.gov. Accessed January 28, 2024. <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2023/3743-odni-releases-intelligence-community-assessment-of-foreign-threats-to-the-2022-u-s-elections>.
- Pappalardo, David. 2022. "'Win the War before the War?': A French Perspective on Cognitive Warfare." War on the Rocks. August 1, 2022. <https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/>.

- Permanent Court of Arbitration. 2016. "The South China Sea Arbitration (the Republic of Philippines v. the People's Republic of China)." Pca-Cpa.org. Permanent Court of Arbitration. 2016. <https://pca-cpa.org/en/cases/7/>.
- Pilger, Michael. 2016. "ADIZ Update: Enforcement in the East China Sea, Prospects for the South China Sea, and Implications for the United States." *U.S.-China Economic and Security Review Commission*. USCC. https://www.uscc.gov/sites/default/files/Research/ADIZ%20Update_0.pdf.
- Pomerleau, Mark. 2023. "How Army Leaders Envision Non-Kinetic Capabilities Enabling Traditional Forces." *DefenseScoop*. September 19, 2023. <https://defensescoop.com/2023/09/19/how-army-leaders-envision-non-kinetic-capabilities-enabling-traditional-forces/>.
- "Qualitative Study Design: Grounded Theory." 2023. *Deakin.libguides.com*. October 12, 2023. <https://deakin.libguides.com/qualitative-study-designs/grounded-theory>.
- Review of *Tips on Qualitative & Quantitative Data Collection Methods*. 2007. In *Sites*. May 2007. http://www.insites.org/CLIP_v1_site/downloads/PDFs/TipsQualQuanMthds.4B.8-07.pdf.
- Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus & Giroux.
- Robbins, Joseph. 2020. "Countering Russian Disinformation." *Www.csis.org*. September 23, 2020. <https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation>.
- Rondeaux, Candace, and David Serman. 2019. "Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World." *New America*. February 20, 2019. <https://www.newamerica.org/future-security/reports/twenty-first-century-proxy-warfare-confronting-strategic-innovation-multipolar-world/>.
- Rumer, Eugene. 2019. "The Primakov (Not Gerasimov) Doctrine in Action." *Carnegie Endowment for International Peace*. June 5, 2019. <https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254>.
- Schnauffer, Tad. 2017. "Redefining Hybrid Warfare: Russia's Non-Linear War against the West." *Journal of Strategic Security* 10, no. 1 (March): 17–31. <https://doi.org/10.5038/1944-0472.10.1.1538>.
- Shabbir, Dr. Muhammad. 2023. "Primakov Doctrine and Russian Foreign Policy." *Insight G&RS-10*, no. 2958-5735 (March): 1–3. <https://ndu.edu.pk/issra/pub/insight/PrimakovDoctrine/PRIMAKOV-DOCTRINE.pdf>.

- Shelbourne, Mallory, and Sam Lagrone. 2024. "China's Attacks on Philippine Resupply Missions Test 70-Year-Old Defense Pact." USNI News. U.S. Naval Institute. March 29, 2024. <https://news.usni.org/2024/03/29/chinas-attacks-on-philippine-resupply-missions-test-70-year-old-defense-pact>.
- Smith, M. E. (2016). Hybrid warfare and its implications for defense and security policies. *European View*, 15(2), 223-234.
- Takagi, Koichiro. 2022. "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine." *War on the Rocks*. July 22, 2022. <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/>.
- Thomas, Clayton. 2020. "U.S. Killing of Qasem Soleimani: Frequently Asked Questions." *Congressional Research Service*. U.S. Congress. https://www.everycrsreport.com/files/20200108_R46148_55dabd56f9a6784bd8e780cf9dcb9028c01a76cf.pdf?fbclid=IwAR1mPdKPmuXYNqTtpICkHkEjXhfoPzAnuAjqLP71r3I6i6DHhRHkqHblPes.
- Trochim, William M.K. n.d. "The Research Methods Knowledge Base - Qualitative Measures." *Conjointly.com*. Conjoint.ly. Accessed February 22, 2024. <https://conjointly.com/kb/qualitative-measures/>.
- "Warfighting." 1997. U.S. Marine Corps Website. Department of the Navy. June 20, 1997. <https://www.marines.mil/Portals/1/Publications/MCDP%201%20Warfighting.pdf>.
- "What Is Irregular Warfare." n.d. Irregular Warfare Technical Support Directorate (IWTSD Website). Accessed February 10, 2024. <https://www.cttso.gov/About.html>.
- Yadav, Kamyia, Martin J. Riedel, Alicia Wanless, and Samuel Woolley. 2023. "What Makes an Influence Operation Malign?" *Carnegie Endowment for Peace*. August 7, 2023. <https://carnegieendowment.org/2023/08/07/what-makes-influence-operation-malign-pub-90323>.
- Yuriy Danyk, and Chad M Briggs. 2023. "Modern Cognitive Operations and Hybrid Warfare." *Journal of Strategic Security* 16, no. 1 (April): 35–50. <https://doi.org/10.5038/1944-0472.16.1.2032>.